

Puerta de enlace Wireless Cable Gateway CG3300CMR

Manual del usuario



350 East Plumeria Drive
San José, CA 95134
EE. UU.

Agosto de 2012
202-11089-01
v1.0

Servicio técnico

Gracias por elegir NETGEAR. Para registrar el producto, obtener las últimas actualizaciones o acceder al servicio de asistencia técnica en línea, visite http://support.netgear.com.

Teléfono (sólo EE. UU. y Canadá): 1-888-NETGEAR.

Teléfono (resto de países): consulte la ficha de información de servicio técnico.

Marcas comerciales

NETGEAR, el logotipo de NETGEAR y Connect with Innovation son marcas comerciales o marcas comerciales registradas de NETGEAR, Inc. o sus filiales en Estados Unidos y otros países. La información contenida en el documento puede sufrir modificaciones sin previo aviso. El resto de marcas y nombres de productos son marcas comerciales o marcas comerciales registradas de sus respectivos titulares. © 2012 NETGEAR, Inc. Todos los derechos reservados.

Condiciones

Con el fin de mejorar el diseño interno, el funcionamiento y la fiabilidad, NETGEAR se reserva el derecho a modificar el producto descrito en el presente documento sin previo aviso. NETGEAR no asume responsabilidad alguna derivada del uso o la aplicación de los productos o circuitos descritos en el presente documento.

Contenido

Capítulo 4 Seguridad

Capítulo 5 Administración

Capítulo 6 Configuración avanzada

Capítulo 7 Solución de problemas

Apéndice A Información complementaria

Apéndice B Notificación de cumplimiento

Índice alfabético

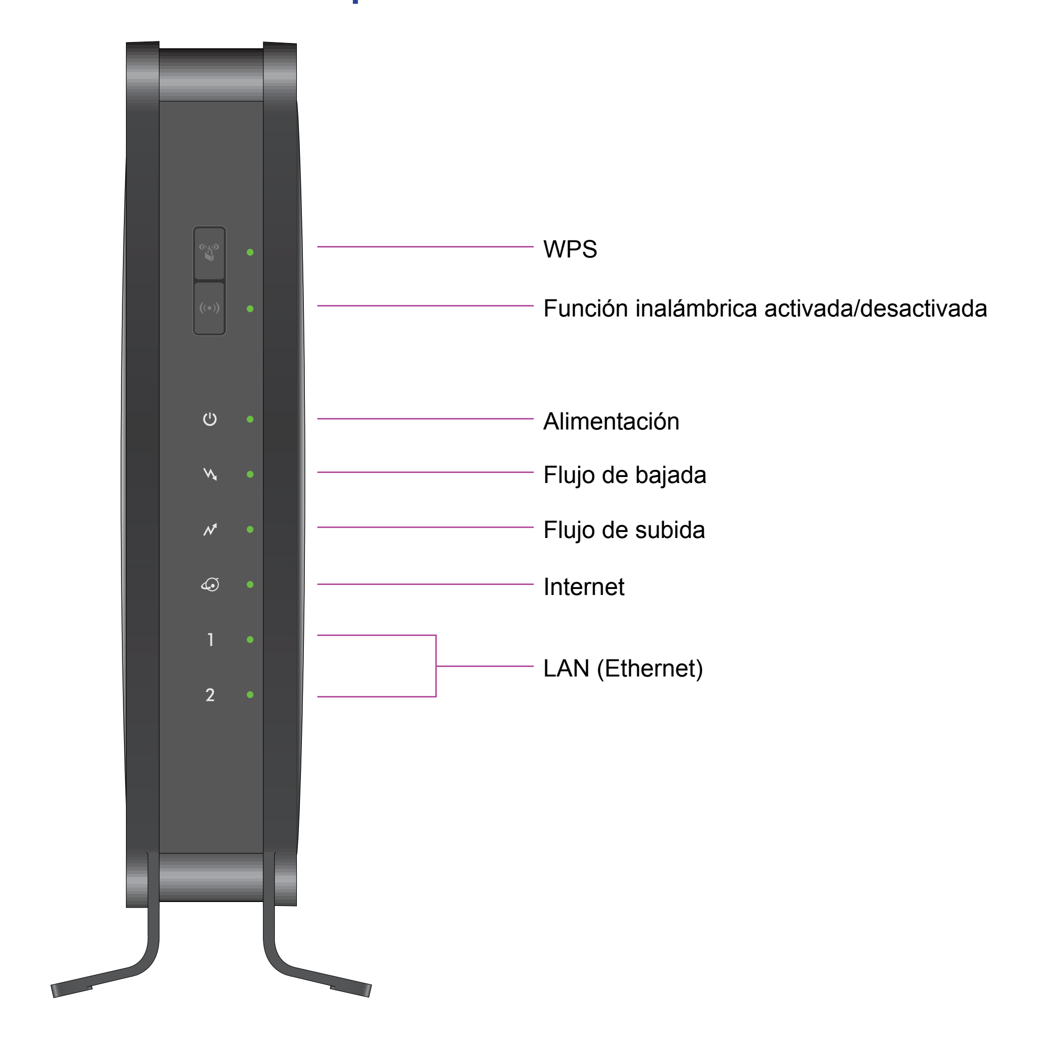
1 Conexión a la puerta de enlace

Introducción a la puerta de enlace

En este capítulo se describe cómo configurar la conexión a Internet de la puerta de enlace. Consta de las siguientes secciones:

Nota: Para obtener más información sobre los temas que se tratan en este manual, visite el sitio web de servicio técnico en *support.netgear.com*.

Panel frontal de la puerta de enlace



Nota: Para obtener el mejor rendimiento, coloque la puerta de enlace verticalmente en el soporte. No instale esta unidad en una pared, no está diseñada para montaje en pared.

Los indicadores sirven para comprobar los diferentes estados y conexiones. En la siguiente tabla se enumeran y describen todos los indicadores LED y botones que se encuentran en el panel frontal de la puerta de enlace.

Indicador	Descripción
Alimentación	• **Verde**. El cable módem recibe corriente. • **Intermitente**. Diagnóstico automático del encendido. • **Apagado**. Sin corriente.
Flujo de bajada	• **Verde**. Hay más de un canal bloqueado (agrupación de canales). • **Ámbar**. Un canal está bloqueado (sin agrupación de canales). • **Intermitente**. La unidad busca un canal de flujo de bajada. • **Apagado**. No hay ningún canal de flujo de bajada bloqueado.
Flujo de subida	• **Verde**. Hay más de un canal bloqueado (agrupación de canales). • **Ámbar**. Un canal está bloqueado (sin agrupación de canales). • **Intermitente**. La unidad busca un canal de flujo de subida. • **Apagado**. No hay ningún canal de flujo de subida bloqueado.
Internet	• **Verde fijo**. El cable módem está conectado. • **Intermitente**. El cable módem se está sincronizando con el CMTS del proveedor de cable. • **Apagado**. El cable módem está desconectado.
2 LAN (Ethernet)	Verde: 1.000 Mbps. Ámbar: 100/10 Mbps. • **Fijo**. Hay un dispositivo Ethernet conectado y encendido. • **Intermitente**. Se están transmitiendo o recibiendo datos a través del puerto Ethernet. • **Apagado**. No se ha detectado un dispositivo Ethernet conectado al puerto Ethernet.
Botón	**Descripción**
WPS	Si se pulsa este botón, la puerta de enlace establece conexión, durante un periodo de tiempo de 2 minutos, con otros dispositivos compatibles con WPS. **Nota**: Se ha desactivado WPS.
Función inalámbrica activada/ desactivada)	Activa y desactiva la radio inalámbrica de la puerta de enlace. La radio inalámbrica está activada por defecto. El LED situado debajo del botón indica si la radio inalámbrica está o no activada. **Nota**: Se ha desactivado el botón de función inalámbrica activada/desactivada.

Panel posterior de la puerta de enlace



El panel posterior incluye las siguientes conexiones, vistas de arriba a abajo:

- **2 puertos LAN Ethernet Gigabit**. Utilice estos puertos para la conexión con equipos locales.
- **Botón de restauración de la configuración de fábrica**. Puede restablecer la puerta de enlace a la configuración predeterminada de fábrica. Mantenga pulsado el botón de **restauración de la configuración de fábrica** durante más de 7 segundos. La puerta de enlace se reinicia y se restablece la configuración predeterminada de fábrica. Consulte *Configuración predeterminada de fábrica* en la página 78.
- **Conector de cable coaxial**. Conecte un cable coaxial a la conexión del proveedor de servicios de cable.
- **Entrada de la fuente de alimentación**. Conecte aquí la unidad de la fuente de alimentación.
- **Botón de encendido y apagado.** Púlselo para encender. Púlselo de nuevo para apagar.

Modelos y fabricantes de fuentes de alimentación

Nota: Utilice solo fuentes de alimentación que se indique en el *Manual del usuario*.

- Adaptador de CWT
  Fabricante: Channel Well Technology Co Ltd
  Modelo: SAL018F2
- Adaptador de PI
  Fabricante: PI Electronics (H.K.) Ltd.
  Modelo: AD817000

Etiqueta de la puerta de enlace

La etiqueta situada en la parte inferior de la puerta de enlace muestra los datos de WPS PIN, inicio de sesión , la dirección MAC y el número de serie.



Inicio de sesión en la puerta de enlace

Puede iniciar sesión en la puerta de enlace para ver o cambiar la configuración.

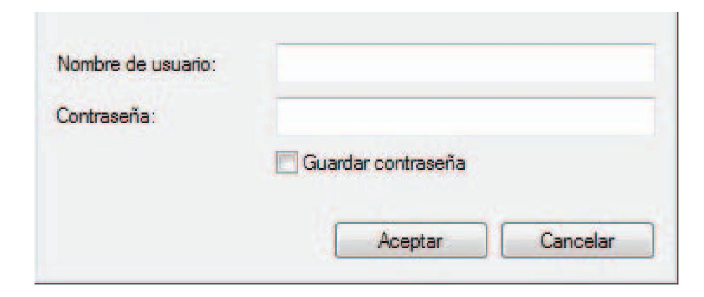
Nota: Para conectarse a la puerta de enlace, utilice un equipo configurado para DHCP (la mayoría de los equipos lo están). Para obtener ayuda sobre la configuración DHCP, consulte las instrucciones incluidas con el equipo.

La puerta de enlace le desconectará automáticamente tras cinco minutos de inactividad.

➢ **Para iniciar sesión en el puerta de enlace:**

1. En el equipo que está conectado a la puerta de enlace mediante un cable Ethernet, escriba **http://192.168.1.1** en el campo de dirección del navegador de Internet.

   Se abrirá una ventana de inicio de sesión.



2. Inicie sesión con **admin** como nombre de usuario y la contraseña predeterminada **password**.

   Cuando se conecte (consulte *Pantalla de inicio Básico* en la página 12), aparecerá la pantalla de inicio Básico de la puerta de enlace.

Ver las pantallas de inicio de la puerta de enlace

Las pantallas de inicio de la puerta de enlace incluye la pantalla de inicio Básico y una pantalla de inicio Avanzado.

Pantalla de inicio Básico

Al conectarse a la puerta de enlace, aparece el panel (pantalla de inicio Básico) de la puerta de enlace.



Menús (Haga clic en la pestaña Avanzado para ver más)

La pantalla de inicio Básico de la puerta de enlace tiene un panel que le permite ver el estado de su conexión a Internet y a la red de un solo vistazo. Puede hacer clic en cualquiera de los apartados del panel para ver información más pormenorizada. La columna izquierda tiene los menús y, en la parte superior, hay una pestaña Avanzado que se utiliza para acceder a otros menús y pantallas.

- **Inicio**. Esta pantalla de panel aparecerá cuando se conecte a la puerta de enlace o seleccione la pestaña Inicio.
- **Conexión**. Vea o modifique la configuración inalámbrica de la puerta de enlace.
- **Dispositivos vinculados**. Vea los dispositivos conectados a su red.
- **Red de invitados**. Configure una red de invitados para que los visitantes puedan utilizar la conexión a Internet de la puerta de enlace.

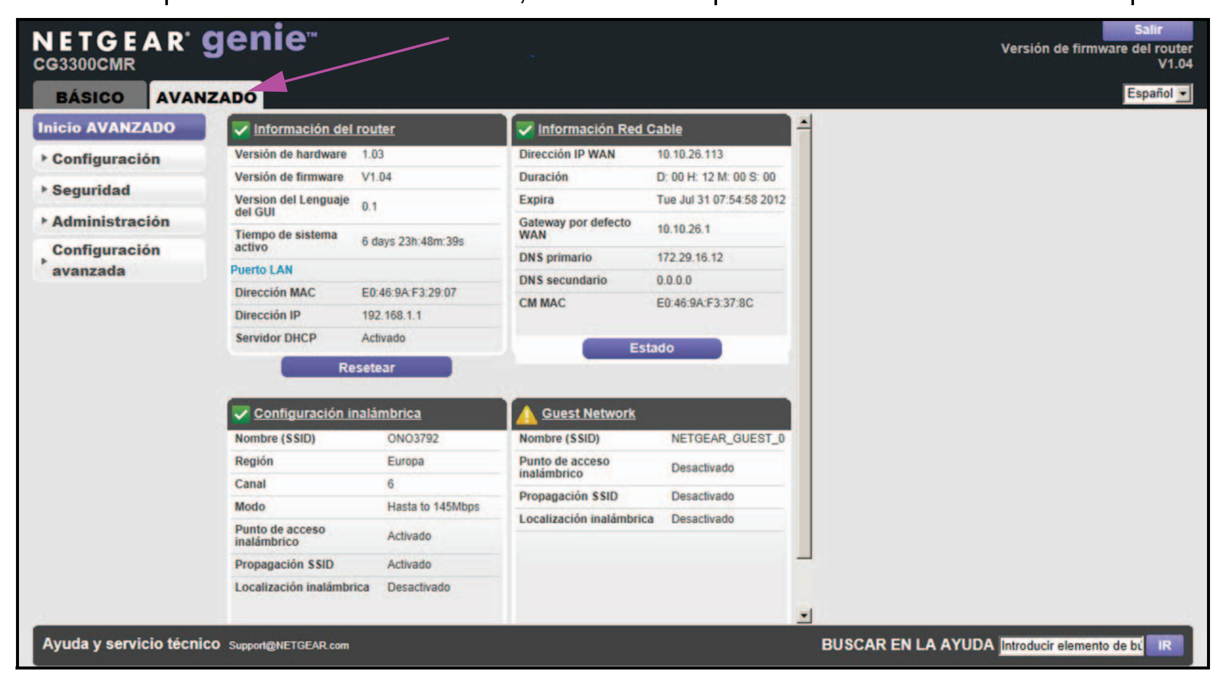
- **Pestaña Avanzado**. Configure la puerta de enlace para situaciones excepcionales, por ejemplo, si se necesita acceso remoto mediante un nombre de dominio o una IP. Consulte *Pantalla de inicio Avanzado* en la página 13. El uso de esta pestaña exige un profundo conocimiento de los conceptos de redes.

Para obtener más información acerca de la configuración básica, consulte el *Capítulo 2, Configuración básica del asistente genie*.

Pantalla de inicio Avanzado

Nota: El uso de esta pantalla de inicio Avanzado exige un profundo conocimiento de los conceptos de redes.

Para ver la pantalla de inicio Avanzado, seleccione la pestaña **Avanzado** del menú superior.



La pantalla de inicio Avanzado de la puerta de enlace tiene un panel que le permite ver la configuración de la puerta de enlace y la red de un solo vistazo. Puede hacer clic en cualquiera de los apartados del panel para ver información más pormenorizada. La columna izquierda tiene los menús y, en la parte superior, está la pestaña Básico que se utiliza para acceder a los menús y pantallas básicos.

- **Inicio Avanzado**. Esta pantalla de panel aparece al seleccionar la pestaña Avanzado.
- **Configuración**. Configure la conexión a Internet, la conexión inalámbrica, la red de invitados, la WAN y la LAN.
- **Seguridad**. Bloquear sitios, bloquear servicios y configurar notificaciones por correo electrónico.

- **Administración**. Vea el estado del router, los registros y los logs de eventos, haga una copia de seguridad, restaure el archivo de configuración y cambe la contraseña de la puerta de enlace.
- **Configuración avanzada**. Configure las funciones avanzadas de la red, por ejemplo, el reenvío de puertos, la activación de puertos, el DNS dinámico, el UPnP y el IPv6.
- **Pestaña Inicio**. Regrese a la pantalla de inicio Básico. Consulte *Pantalla de inicio Básico* en la página 12.

Para obtener más información acerca de la configuración avanzada, consulte el apartado *Capítulo 3, Inicio Avanzado del asistente genie*.

Añadir equipos o dispositivos inalámbricos a la red

Consulte *Redes de invitados* en la página 20 para obtener instrucciones sobre cómo configurar una red de invitados.

➢ **Para añadir equipos o dispositivos inalámbricos a la red:**

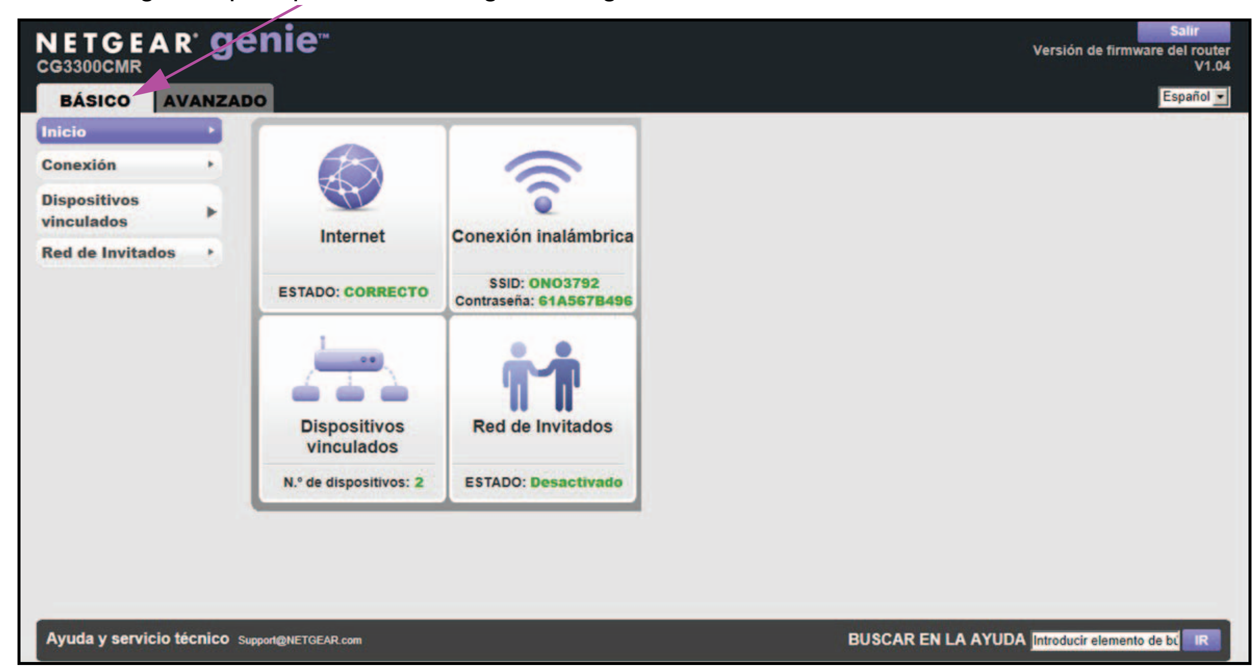
1. Abra la aplicación de software que gestiona sus conexiones inalámbricas en el dispositivo inalámbrico (ordenador portátil, videoconsola, iPhone) que desea conectar a la puerta de enlace. Este software comenzará a buscar las redes inalámbricas disponibles en su zona.
2. Localice su red y selecciónela. Si no cambió el nombre de la red durante el proceso de configuración, busque el nombre de red inalámbrica (SSID) predeterminado y selecciónelo. El SSID predeterminado se encuentra en la etiqueta de la parte inferior de la puerta de enlace.
3. Introduzca la contraseña de la puerta de enlace y haga clic en **Conectar**. La contraseña predeterminada de la puerta de enlace se encuentra en la etiqueta de producto de la parte inferior de la puerta de enlace.
4. Repita los pasos del 1 al 3 para añadir otros dispositivos inalámbricos.

Configuración básica del asistente genie

2

Su conexión a Internet y la red

En este capítulo, se explican las funciones disponibles en la pantalla de inicio Básico del asistente genie que aparece en la siguiente figura:



Este capítulo contiene las siguientes secciones:

- *Conexión inalámbrica*
- *Dispositivos vinculados*
- *Redes de invitados*

Conexión inalámbrica

Nota: A fin de garantizar la conformidad con las normativas y la compatibilidad entre productos similares de su zona geográfica, ajuste correctamente la región y el canal de funcionamiento.

Ubicación del router para obtener la mejor conexión inalámbrica posible

El alcance de la conexión inalámbrica puede variar dependiendo de dónde esté ubicado el router. Para un resultado óptimo, coloque el router:

- Cerca del centro de la zona en la que operan los equipos.
- En un lugar elevado, como una estantería.
- Lejos de posibles focos de interferencias, como equipos, hornos microondas o teléfonos inalámbricos.
- Lejos de grandes superficies metálicas.

Nota: Si no se siguen correctamente las siguientes recomendaciones el rendimiento puede disminuir notablemente, o incluso la conexión a la puerta de enlace puede resultar inviable.

Pantalla Conexión inalámbrica

La pantalla Conexión inalámbrica le permite ver o configurar la red inalámbrica.

La puerta de enlace de cable inalámbrica incluye seguridad predeterminada. Dicha función implica que el nombre de red WiFi (SSID), la clave de red (contraseña) y la opción de seguridad (protocolo de cifrado) vienen predeterminadas de fábrica. Podrá encontrar la contraseña y la SSID predeterminadas en la parte inferior de la unidad.

Nota: La SSID y la contraseña predeterminadas se generan de manera exclusiva para cada dispositivo para proteger y optimizar la seguridad inalámbrica.

NETGEAR le recomienda no modificar los ajustes de seguridad predeterminados. Si decide modificar los ajustes de seguridad predeterminados, tome nota de los nuevos ajustes y guárdelos en un lugar seguro.

Si utiliza un equipo inalámbrico para cambiar el nombre de la red inalámbrica (SSID) u otros ajustes de seguridad inalámbrica, al hacer clic en Aplicar, se desconectará. Para evitarlo, utilice un equipo con una conexión por cable para acceder a la puerta de enlace.

➢ **Para ver o modificar la configuración inalámbrica básica:**

1. En la pantalla de inicio básico, seleccione **Conexión** para acceder a la pantalla Conexión inalámbrica.



Los apartados, ajustes y procedimientos de la pantalla se explican en las siguientes secciones.

2. Cambie lo que necesite y haga clic en **Aplicar** para guardar la configuración.
3. Configure y pruebe los equipos y los dispositivos inalámbricos para asegurarse de que se pueden conectar de forma inalámbrica. De no ser así, compruebe lo siguiente:
   - ¿Está su equipo o dispositivo inalámbrico conectado a su red o a otra red inalámbrica de su zona? Algunos dispositivos inalámbricos se conectan de forma automática a la primera red disponible (sin seguridad inalámbrica) que detectan.
   - ¿Aparece el equipo o dispositivo inalámbrico en la pantalla Dispositivos vinculados? Si es así, estará conectado a la red.
   - Si no está seguro de cuál es el nombre de red (SSID) o la contraseña, mire en la etiqueta de la parte inferior de la puerta de enlace.

Campos de la pantalla Conexión inalámbrica

Red inalámbrica

- **Publicar SSID**. Esta configuración permite a la puerta de enlace emitir su SSID para que las estaciones inalámbricas puedan verlo en sus listas de redes buscadas. De forma predeterminada, esta casilla está activada. Para desactivar la publicación de la SSID, desactive la casilla **Publicar SSID** y haga clic en **Aplicar**.
- **Activar el aislamiento inalámbrico**. Si se ha activado esta casilla de verificación, podrán utilizar Internet los clientes inalámbricos (equipos o dispositivo inalámbricos) que se unan a la red. Sin embargo, no podrán acceder entre sí ni tampoco a los dispositivos Ethernet de la red.
- **Nombre (SSID)**. La SSID también se denomina nombre de red inalámbrica. Introduzca un nombre de 32 caracteres (máximo) en este campo. Tenga en cuenta que este campo distingue entre mayúsculas y minúsculas. La SSID predeterminada se genera de manera aleatoria y ***NETGEAR recomienda encarecidamente no modificarla***.
- **Región**. El lugar en el que se utiliza la puerta de enlace.
- **Canal**. Este ajuste es el canal inalámbrico que utiliza la puerta de enlace. Seleccione un valor del 1 al 13. (Para productos del mercado estadounidense, solo se pueden utilizar los canales del 1 al 11). No modifique el canal salvo que experimente interferencias (por ejemplo, la pérdida de conexiones o lentitud en las transferencias de datos). Si se produce alguna interferencia, experimente con diferentes canales para ver cuál es el mejor.
- **Modo**. Hasta 145 Mbps es el valor predeterminado y permite que se unan a la red dispositivos inalámbricos de 802.11n y 802.11g. g & b admite hasta 54 Mbps. El ajuste de 300 Mbps permite que se conecten a esta velocidad los dispositivos 802.11n.

Configuración de Opciones de seguridad

El apartado Opciones de seguridad de la pantalla Conexión inalámbrica le permite cambiar la opción de seguridad y la contraseña. ***NETGEAR le recomienda no cambiar la contraseña ni la opción de seguridad***, pero si desea cambiar esta configuración, aquí se explica cómo hacerlo.

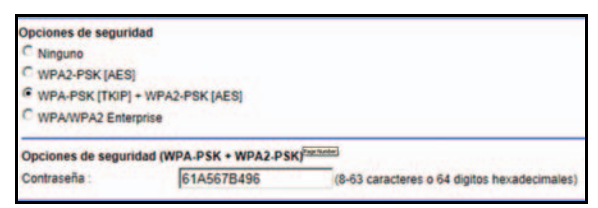


CUIDADO:

No desactive la seguridad.

➤ **Para cambiar la contraseña y la opción de seguridad de WPA:**

1. En Opciones de seguridad, seleccione la opción de WPA que desee.



2. En el campo Contraseña que aparece cuando se selecciona una opción de seguridad WPA, introduzca la clave de red (contraseña) que desee utilizar. Es una cadena de texto de 8 a 63 caracteres.

Dispositivos vinculados

Aquí, puede ver todos los equipos o dispositivos que están conectados actualmente a la red. En la pantalla de inicio Básico, seleccione **Dispositivos vinculados** para acceder a la siguiente pantalla:



Los dispositivos con cables se conectan a la puerta de enlace mediante cables Ethernet. Los dispositivos inalámbricos se han unido a la red inalámbrica.

- **Dirección IP**. La dirección IP que la puerta de enlace asignó a este dispositivo cuando se unió a la red. Este número puede variar si un dispositivo se desconecta de la red y vuelve a conectarse a ella.
- **Nombre del dispositivo**. Si se conoce el nombre del dispositivo, aparecerá aquí.

Puede hacer clic en **Actualizar** para actualizar esta pantalla.

Redes de invitados

Puede añadir una red de invitados para que las personas que le visiten puedan utilizar Internet sin facilitarles la clave de seguridad inalámbrica.

➤ **Para configurar una red de invitados:**

1. Seleccione **Básico > Red de invitados** para acceder a la siguiente pantalla:



2. Seleccione cualquiera de los siguientes ajustes inalámbricos:

   Activar la red invitada. Si se ha activado esta casilla, la red de invitados estará activa y los invitados podrán conectarse a la red sin utilizar la SSID de este perfil.

   Activar emisión de la SSID. Si esta casilla está activada, el repetidor inalámbrico publica su nombre (SSID) a todas las estaciones inalámbricas. A continuación, las estaciones que no dispongan de una SSID podrán seleccionar la SSID correspondiente para conectarse a este repetidor.

   - **Activar el aislamiento inalámbrico**. Si se ha activado esta casilla de verificación, podrán utilizar Internet los clientes inalámbricos (equipos o dispositivo inalámbricos) que se unan a la red. Sin embargo, no podrán acceder entre sí ni tampoco a los dispositivos Ethernet de la red.

3. Asigne un nombre a la red de invitados.

   El nombre de la red de invitados distingue entre mayúsculas y minúsculas, y puede tener hasta 32 caracteres. Después, configure manualmente los dispositivos inalámbricos de la red para utilizar el nombre de la red de invitados además de la SSID principal.

4. Seleccione el grupo de la red de invitados de la lista.
5. Seleccione una opción de seguridad de la lista. Las opciones de seguridad se describen en *Opciones de seguridad inalámbrica de la red de invitados* en la página 21.
6. Haga clic en **Aplicar** para guardar lo que ha seleccionado.

Opciones de seguridad inalámbrica de la red de invitados

Una opción de seguridad es el tipo de protocolo de seguridad aplicado a la red inalámbrica. El protocolo de seguridad en vigor cifra las transmisiones de datos y garantiza que solo los dispositivos seguros reciban autorización para conectarse a la red.

Esta sección presenta un resumen de las opciones de seguridad y ofrece orientación sobre cuándo utilizar cada una de las opciones. También se puede configurar una red de invitados sin seguridad inalámbrica. NETGEAR *no* recomienda prescindir de la seguridad inalámbrica.

El cifrado Wi-Fi Protected Access (WPA) se encuentra integrado en todos los hardware que tienen el sello de certificación Wi-Fi. Este sello significa que el producto cumple el único estándar mundial para redes de área local inalámbricas de alta velocidad que ha establecido la Wi-Fi Alliance (*http://www.wi-fi.org/*).

WPA-PSK emplea una contraseña para realizar la autenticación y generar las claves de cifrado de datos iniciales. A continuación, varía de forma dinámica la clave de cifrado. WPA-PSK utiliza un cifrado de datos de protocolo de integridad de claves temporal (TKIP) y aplica la mayor parte del estándar IEEE 802.11i. Se ha diseñado para funcionar con todas las tarjetas de interfaz de redes inalámbricas. No todos los repetidores inalámbricos funcionan con este estándar. WPA2-PSK sustituye a WPA-PSK.

WPA2-PSK es más sólido que WPA. Según se ha anunciado, en teoría, es indescifrable, dado el mayor nivel de aleatoriedad de las claves de cifrado que genera. WPA2-PSK consigue una mayor velocidad porque se implementa a través de hardware, mientras que WPA-PSK se implementa mediante software. WPA2-PSK emplea una contraseña para autenticar y generar las claves de cifrado de datos iniciales. A continuación, varía de forma dinámica la clave de cifrado.

El modo mixto WPA-PSK + WPA2-PSK puede ofrecer una mayor compatibilidad con todos los clientes inalámbricos. Los clientes WPA2-PSK logran mayor velocidad y seguridad, y los clientes WPA-PSK consiguen una velocidad y seguridad aceptables. La documentación que acompaña al adaptador inalámbrico y el software de cliente WPA incluye instrucciones de configuración de sus parámetros WPA.

Inicio Avanzado del asistente genie

3

Especificación de la configuración personalizada

En este capítulo, se explican las funciones disponibles en la pantalla de inicio Avanzado del asistente genie que aparece en la siguiente ilustración:



Este capítulo contiene las siguientes secciones:

- *Menú Configuración*
- *Configuración WAN*
- *Configuración LAN*

Algunas de las opciones seleccionadas en la pantalla de inicio Avanzado se describen en otras secciones:

- **Seguridad**. Consulte el *Capítulo 4, Seguridad*.
- **Administración**. Consulte el *Capítulo 5, Administración*.
- **Configuración avanzada**. Consulte el *Capítulo 6, Configuración avanzada*.

Menú Configuración

Seleccione **Avanzado > Configuración** para visualizar el menú Configuración. Estarán disponibles las siguientes opciones:

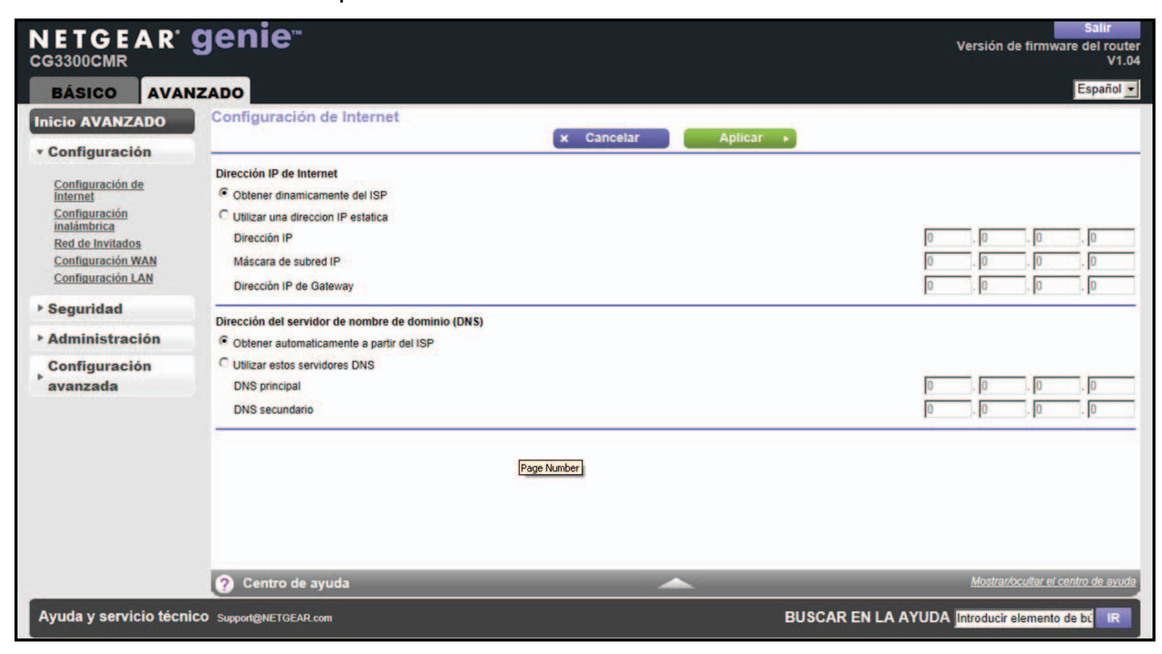
- **Configuración de Internet**. Consulte *Configuración de Internet* en la página 24.
- **Configuración inalámbrica**. Este elemento del menú es un acceso directo a la misma pantalla de conexión a la que se accede desde el panel de la página de inicio Básico. Consulte *Conexión inalámbrica* en la página 16.
- **Red de invitados**. Este elemento del menú es un acceso directo a la misma pantalla de red de invitados a la que se accede desde el panel de la página de inicio Básico. Consulte *Redes de invitados* en la página 20.
- **Configuración WAN**. Configuración de red de área extensa (WAN). Consulte *Configuración WAN* en la página 26.
- **Configuración LAN**. Configuración de red de área local (LAN). Consulte *Configuración LAN* en la página 29.

Configuración de Internet

En la pantalla Configuración de Internet podrá ver o modificar la información del ISP.

➢ **Para cambiar la configuración de Internet:**

1. En la pantalla de inicio Avanzado, seleccione **Configuración > Configuración de Internet**. Se mostrará la pantalla:



2. Introduzca la configuración de la dirección IP y del servidor DNS. En condiciones normales, la configuración predeterminada funciona adecuadamente. Si tiene problemas con la conexión, compruebe la configuración del ISP.
3. Haga clic en **Aplicar** para guardar la configuración.

Campos de la pantalla Configuración de Internet

En las descripciones siguientes, se explican todos los campos que pueden encontrarse en la pantalla Configuración de Internet.

Dirección IP de Internet.

- Si se conecta a su servicio mediante un inicio de sesión o su proveedor no le proporcionó una dirección IP fija, el router asigna automáticamente una dirección IP cuando se conecta. Seleccione **Obtener dinámicamente del ISP.**
- Si dispone de una dirección fija (también denominada estática), su proveedor de servicios de Internet le habrá proporcionado la información necesaria. Seleccione **Utilizar una dirección IP estática** e introduzca la dirección IP, la máscara de subred IP y la dirección IP de la puerta de enlace en los campos correspondientes.

  Por ejemplo:

  - Dirección IP. 24.218.156.183
  - Máscara de subred IP. 255.255.255.0
  - Dirección IP de Gateway. 24.218.156.1

Dirección del servidor de nombre de dominio (DNS). El servidor DNS se utiliza para acceder a direcciones por sus nombres.

- Si su proveedor le proporcionó una o dos direcciones DNS, seleccione **Utilizar estos servidores DNS** y escriba dichas direcciones.
- En caso contrario, seleccione **Obtener automáticamente a partir del ISP**.

Nota: Si aparece el error Dirección no encontrada al intentar acceder a un sitio web, es posible que los servidores DNS no estén configurados correctamente. Póngase en contacto con su proveedor para obtener las direcciones del servidor DNS.

Configuración WAN

En la pantalla Configuración WAN, podrá configurar un servidor DMZ (zona desmilitarizada), cambiar el tamaño de la unidad máxima de transmisión (MTU) y activar la puerta de enlace para que responda a un ping por el puerto WAN (Internet).

➤ **Para cambiar la configuración de la WAN:**

Seleccione **Avanzado > Configuración > Configuración WAN** para ver la siguiente pantalla:



- **Servidor DMZ predeterminado**. Esta función resulta útil en ocasiones cuando se juega en línea o se participa en videoconferencias. Tenga cuidado cuando utilice esta función puesto que resta eficacia a la seguridad del firewall. Consulte el *Servidor DMZ predeterminado* en la página 27 para obtener más información.
- **Responder a ping en el puerto de Internet**. Si desea que la puerta de enlace responda a un ping procedente de Internet, active esta casilla. Utilice esta función únicamente como una herramienta de diagnóstico, ya que permite que se detecte también la puerta de enlace. No active esta casilla a menos que tenga un motivo concreto para hacerlo.
- **Tamaño de la MTU (en bytes)**. El valor de la MTU (unidad máxima de transmisión) habitual en la mayoría de las redes Ethernet es 1500 bytes o 1492 bytes para conexiones PPPoE. Con algunos ISP, reduzca la MTU. Normalmente no tendrá que hacerlo a menos que esté absolutamente seguro de que es necesario para la conexión. Consulte *Cambiar el tamaño de la MTU* en la página 27.

Servidor DMZ predeterminado

La función de servidor DMZ predeterminado resulta útil cuando se están utilizando algunos juegos en línea y aplicaciones de videoconferencia que no son compatibles con la traducción de direcciones de red (NAT). La puerta de enlace está programada para reconocer algunas de estas aplicaciones y para funcionar correctamente con ellas, pero hay otras aplicaciones que no funcionan bien. En algunos casos, un equipo local puede ejecutar correctamente la aplicación si se introduce la dirección IP de ese equipo como servidor DMZ predeterminado.



ADVERTENCIA:

Los servidores DMZ constituyen un riesgo para la seguridad. Un equipo designado como servidor DMZ predeterminado pierde gran parte de la protección del firewall y está expuesto a ataques de Internet. Si la seguridad del equipo del servidor DMZ se ve comprometida, este podrá utilizarse para atacar a otros equipos de su red.

La puerta de enlace bloquea el tráfico entrante de Internet a menos que sea una respuesta a uno de los equipos locales o a un servicio que haya configurado en la pantalla Reenvío de puertos/Activación de puertos. En lugar de bloquear este tráfico, puede hacer que se dirija a un equipo de su red: el servidor DMZ predeterminado.

➤ **Para configurar un servidor DMZ predeterminado:**

1. En la pantalla Configuración WAN, seleccione la casilla **Servidor DMZ predeterminado**.
2. Escriba la dirección IP.
3. Haga clic en **Aplicar**.

Cambiar el tamaño de la MTU

La unidad máxima de transmisión (MTU) es el paquete de datos más grande que transmite un dispositivo de red. Cuando un dispositivo de red se comunica con otro por Internet, los paquetes de datos pasan por muchos dispositivos a lo largo de su recorrido. Si algún dispositivo de la ruta de datos posee un ajuste de MTU inferior al de los demás dispositivos, los paquetes de datos se dividirán (o “fragmentarán”) para ajustarse al dispositivo con la MTU más baja.

El mejor ajuste en cuanto a MTU para el equipo de NETGEAR suele ser el valor predeterminado. Modificar dicho valor suele resolver un problema pero provoca otro diferente. No modifique el tamaño de la MTU salvo que se dé una de estas situaciones:

- Tiene problemas para conectarse al ISP o a otro servicio de Internet y el servicio técnico del ISP o de NETGEAR recomienda cambiar el ajuste de MTU. Estas aplicaciones web suelen exigir un cambio de la MTU:
  - Un sitio web seguro que no se abre o que solo muestra parte de una página web
  - Correo Yahoo

  - Portal de MSN
  - Servicio DSL de America Online
- Utiliza una VPN y tiene graves problemas de rendimiento.
- Ha utilizado un programa para optimizar la MTU por motivos de rendimiento y ahora tiene problemas de funcionamiento o conectividad.

Nota: Un ajuste MTU incorrecto provoca problemas de comunicación por Internet. Entre estos problemas, se encuentran la incapacidad para acceder a determinados sitios web, marcos dentro de los sitios web, páginas de inicio de sesión seguras o servidores FTP o POP.

Si sospecha que tiene un problema con la MTU, una solución habitual es modificar su valor a 1400. Si desea experimentar, puede reducir gradualmente la MTU desde el valor máximo de 1500 hasta que el problema desaparezca. La tabla siguiente describe las aplicaciones y los tamaños de MTU habituales.

Tabla 1. Tamaños habituales de la MTU

MTU	Aplicación
1500	El tamaño de paquete Ethernet máximo y el valor predeterminado. Este tamaño es el valor habitual de conexiones que no es PPPoE ni VPN, y es el valor predeterminado de las NETGEAR, adaptadores y conmutadores NETGEAR.
1492	Se utiliza en entornos PPPoE.
1472	Tamaño máximo de uso para hacer ping. (Los paquetes más grandes se fragmentan).
1468	Se utiliza en algunos entornos DHCP.
1460	Lo puede utilizar AOL si no se tienen archivos adjuntos al correo electrónico de gran tamaño, por ejemplo.
1436	Se utiliza en entornos PPTP o con VPN.
1400	Tamaño máximo para DSL de AOL.
576	Valor habitual para conectarse a los ISP de marcación telefónica.

➤ Para cambiar el tamaño de la MTU:

1. Seleccione **Avanzado > Configuración > Configuración WAN**.
2. En el campo Tamaño de la MTU, introduzca un nuevo tamaño desde 64 a 1500.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración LAN

La pantalla Configuración LAN le permite configurar servicios de la LAN como, por ejemplo, la dirección IP de la puerta de enlace y DHCP. Los valores predeterminados de TCP/IP y DHCP funcionan adecuadamente en la mayoría de los casos.

La puerta de enlace se facilita preconfigurada para utilizar direcciones IP privadas en la LAN y actuar como servidor DHCP. La configuración IP de la LAN predeterminada de la puerta de enlace es:

- Dirección IP de la LAN. **192.168.1.1**
- Máscara de subred. **255.255.255.0**

Estas direcciones forman parte del intervalo de direcciones privadas designado para su uso en redes privadas y resultan adecuadas para la mayoría de las aplicaciones. Si su red le exige que utilice una configuración de direcciones IP diferente, realice los cambios necesarios en la pantalla Configuración LAN.

➤ **Para cambiar la configuración de la LAN:**

Nota: Si cambia la dirección IP de la LAN de la puerta de enlace mientras está conectado a través del navegador, se le desconectará. Abra una nueva conexión a la nueva dirección IP y vuelva a iniciar sesión.

1. Seleccione **Avanzado > Configuración > Configuración LAN** para ver la siguiente pantalla:



2. Introduzca los ajustes que desee personalizar. Estos ajustes se describen en la siguiente sección, *Ajustes de la pantalla Configuración LAN*.
3. Haga clic en **Aplicar** para guardar los cambios.

Ajustes de la pantalla Configuración LAN

Configuración TCP/IP LAN

- **Dirección IP**. La dirección IP de la LAN de la puerta de enlace.
- **Máscara de subred IP**. La máscara de subred de la LAN de la puerta de enlace. Cuando se combina con la dirección IP, la máscara de subred IP permite a un dispositivo saber lo siguiente:
  - Otras direcciones que son locales para él
  - Otras direcciones que se han conectado a través de una puerta de enlace

Utilizar router como servidor DHCP

Esta casilla se selecciona para que la puerta de enlace funcione como un servidor de protocolo de configuración dinámica de host (DHCP).

- **Dirección IP de inicio**. Especifique el inicio del intervalo del grupo de direcciones IP de la misma subred que la puerta de enlace.
- **Dirección IP de destino**. Especifique el fin del intervalo del grupo de direcciones IP de la misma subred que la puerta de enlace.

Reserva de una dirección IP

Si reserva una dirección IP para un equipo de la LAN, dicho equipo recibirá la misma dirección IP cada vez que acceda al servidor DHCP de la puerta de enlace. Asigne direcciones IP reservadas a los servidores que requieran una configuración IP permanente.

Utilizar la puerta de enlace como servidor DHCP

De forma predeterminada, la puerta de enlace funciona como un servidor DHCP. Esta capacidad permite a la puerta de enlace asignar direcciones IP, de servidor DNS y de puerta de enlace predeterminada a todos los equipos conectados a la LAN que se conecten a la puerta de enlace. La dirección de puerta de enlace predeterminada asignada es la dirección LAN de la puerta de enlace. La puerta de enlace asigna direcciones IP a los equipos conectados desde un grupo de direcciones especificadas en esta pantalla. Cada dirección del grupo se probará antes de asignarse para evitar direcciones duplicadas en la LAN. Con la mayoría de las aplicaciones, los ajustes DHCP y TCP/IP predeterminados de la puerta de enlace son satisfactorios.

Podrá especificar el grupo de direcciones IP que se pueden asignar estableciendo la dirección IP de inicio y la dirección IP de destino. Estas direcciones forman parte de la misma subred de direcciones IP que la LAN que está conectada a la puerta de enlace. Mediante la configuración de direcciones predeterminadas, se define un intervalo entre 192.168.1.2 y 192.168.1.254. Podrá reservar parte de este intervalo para dispositivos con direcciones fijas.

La puerta de enlace ofrece los siguientes parámetros a cualquier dispositivo LAN que solicite DHCP:

- Una dirección IP del intervalo que haya definido
- Máscara de subred
- Dirección IP de la puerta de enlace (la dirección IP de la LAN de la puerta de enlace)
- Servidor DNS principal (si introdujo una dirección DNS principal en la pantalla Configuración de Internet; si no es así, la dirección IP de la LAN de la puerta de enlace)
- Servidor DNS secundario (si introdujo una dirección DNS secundaria en la pantalla Configuración de Internet)

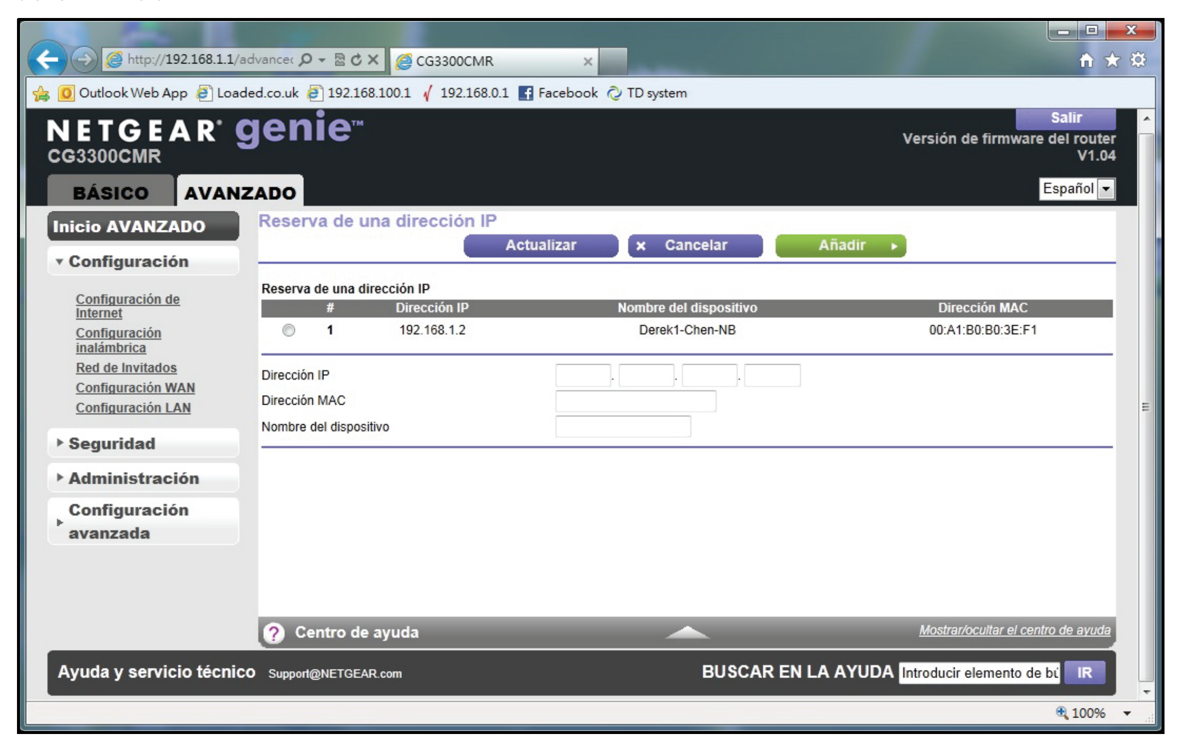
Para utilizar otro dispositivo de la red como servidor DHCP o para configurar manualmente los ajustes de red de todos sus equipos, desactive la casilla **Utilizar router como servidor DHCP** y haga clic en **Aplicar**. De lo contrario, deje esta casilla activada. Si no se ha activado este servicio y no hay otro servidor DHCP disponible en la red, configure las direcciones IP de su equipo manualmente u otros dispositivos no podrán acceder a la puerta de enlace.

Reserva de una dirección IP

Si reserva una dirección IP para un equipo de la LAN, dicho equipo recibirá siempre la misma dirección IP cada vez que acceda al servidor DHCP de la puerta de enlace. Asigne direcciones IP reservadas a los equipos o servidores que requieran una configuración IP permanente.

Para reservar una dirección IP:

1. En el apartado Reserva de emisión de la pantalla Configuración LAN, haga clic en el botón **Añadir**.



2. En el campo Dirección IP, escriba la dirección IP que asignar al equipo o servidor. (Seleccione una dirección IP de la subred de la LAN de la puerta de enlace, por ejemplo, 192.168.1.x.).
3. Escriba la dirección MAC del equipo o del servidor.

Consejo: Si el equipo ya se encuentra en la red, copie su dirección MAC de la pantalla Dispositivos vinculados y péguela aquí.

4. Haga clic en **Aplicar** para introducir la dirección reservada en la tabla.

   La dirección reservada no se asigna hasta que el equipo se pone de nuevo en contacto con el servidor DHCP de la puerta de enlace. Resetee el equipo o acceda a su configuración IP y fuerce una liberación y renovación de DHCP.

Para editar o eliminar una entrada de dirección reservada, seleccione el botón de opción que esté al lado de la dirección reservada que desee editar o eliminar. A continuación, haga clic en **Editar** o **Eliminar**.

Seguridad

4

Cómo mantener el contenido no deseado fuera de la red

En este capítulo, se explica cómo impedir que el contenido no deseado llegue a los equipos y otros dispositivos conectados a la red.

Este capítulo contiene las siguientes secciones:

- *Bloqueo del tráfico HTTP mediante palabras claves*
- *Bloquear servicios (filtrado de puertos)*
- *Notificaciones por correo electrónico de eventos de seguridad*

Bloqueo del tráfico HTTP mediante palabras claves

Utilice el bloqueo mediante palabras clave para impedir que accedan a su red determinados tipos de tráfico HTTP.

1. Seleccione **Avanzado > Seguridad > Bloquear sitios** para acceder a la siguiente pantalla:



2. Seleccione una de las opciones de bloqueo mediante palabras clave:
   - **Nunca**. Desactivar el bloqueo mediante palabras clave.
   - **Siempre**. Activar el bloqueo mediante palabras clave.
3. En el campo de palabra clave, introduzca una palabra clave o dominio, haga clic en **Añadir palabra clave** y haga clic en **Aplicar**.

   La lista de palabras clave admite hasta 32 entradas. Estas son algunas entradas de ejemplo:
   - Especifique XXX para bloquear http://www.badstuff.com/xxx.html.
   - Especifique .com si desea permitir solo sitios con sufijos de dominio tales como .edu o .gov.
   - Introduzca un punto (**.**) para bloquear todo el acceso a la navegación por Internet.

➢ **Para eliminar una palabra clave o un nombre de dominio:**

1. Seleccione la palabra clave que desea eliminar de la lista.
2. Haga clic en **Eliminar palabra clave** y, a continuación, en **Aplicar** para guardar los cambios.

➢ **Para especificar un equipo seguro:**

Puede excluir un equipo seguro del bloqueo y registro. El equipo que excluya tendrá que poseer una dirección IP fija.

1. Seleccione **Permitir a la dirección IP de confianza visitar los sitios bloqueados**.
2. En el campo Dirección IP de confianza, introduzca la dirección IP.
3. Haga clic en **Aplicar** para guardar los cambios.

Bloquear servicios (filtrado de puertos)

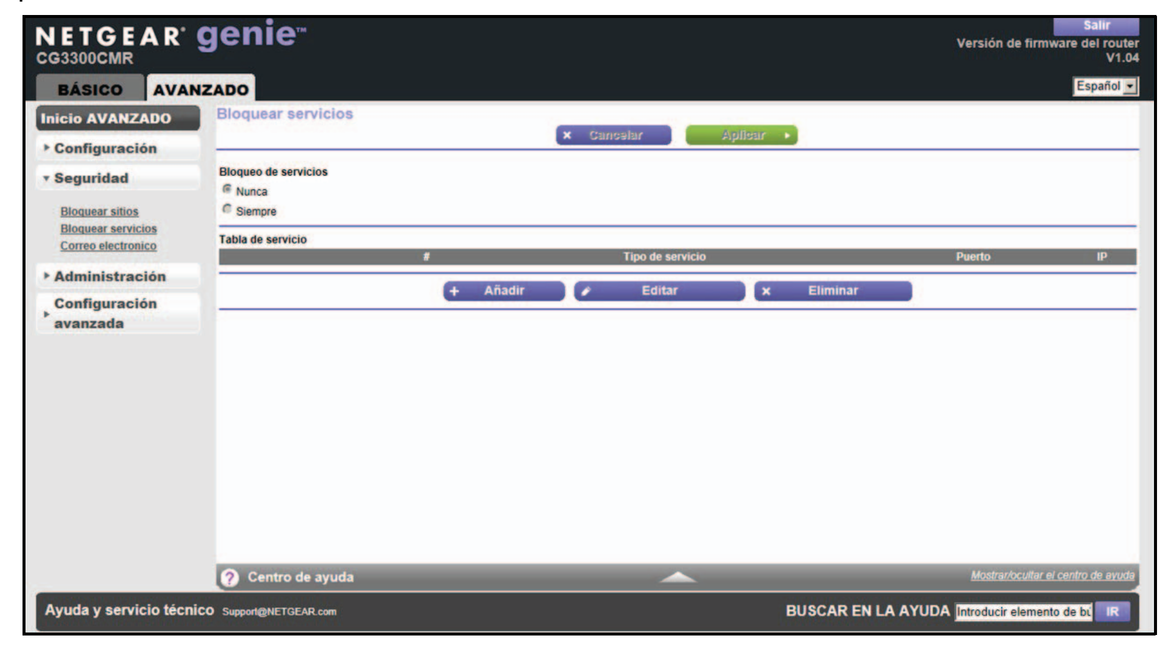
Los equipos de servidor prestan servicios a petición de los equipos de cliente. Por ejemplo, los servidores web dan servicio a las páginas web, los servidores de hora ofrecen información de fecha y hora, y los hosts de juegos ofrecen datos sobre los movimientos de los demás jugadores. Si un equipo de Internet envía una solicitud de servicio a un servidor, un número de puerto o servicio identificará el servicio solicitado. Este número aparecerá como número de puerto de destino de los paquetes IP transmitidos. Por ejemplo, un paquete que se envía con el número de puerto de destino 80 es una solicitud HTTP (servidor web).

Los números de servicio de muchos protocolos comunes son definidos por el Internet Engineering Task Force (IETF en *http://www.ietf.org/*) y publicados en RFC1700, “Assigned Numbers”. Normalmente, los autores de la aplicación eligen los números de servicio de otras aplicaciones del intervalo comprendido entre 1024 y 65535. Aunque la puerta de enlace ya cuenta con una lista de muchos números de puerto del servicio, no solo dispone de estas opciones. Con frecuencia, para conocer la información del número de puerto, podrá ponerse en contacto con el autor de la aplicación o bien preguntar a grupos de usuarios o grupos de noticias, o buscarlo.

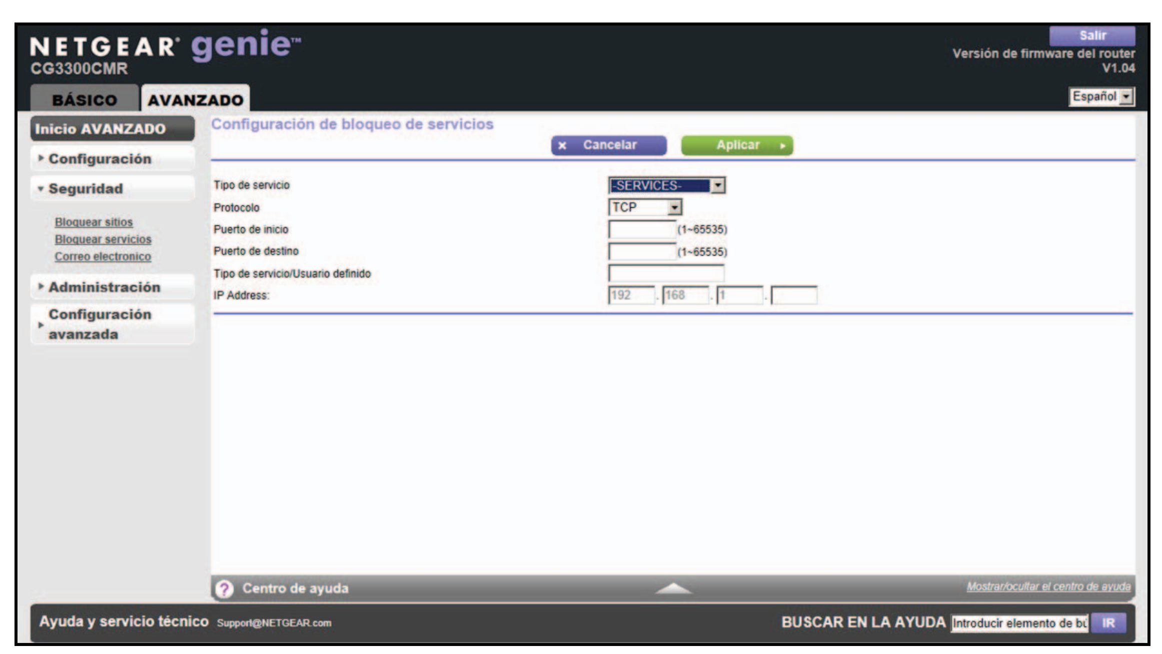
La pantalla Bloquear servicios le permite añadir y bloquear servicios de Internet específicos por equipos de la red. Esta capacidad se denomina bloqueo de servicios o filtrado de puertos. Para añadir un servicio que desee bloquear, determine en primer lugar qué número o intervalo de números de puerto utiliza la aplicación.

➢ Para bloquear servicios:

1. Seleccione **Avanzado > Seguridad > Bloquear servicios** para acceder a la siguiente pantalla:



2. Seleccione una de las opciones de bloqueo de servicios:
   - **Nunca**. Desactivar el bloqueo de servicios.
   - **Siempre**. Activar el bloqueo de servicios.
3. Haga clic en **Añadir** para añadir un servicio. Aparecerá la pantalla Configuración de bloqueo de servicios:



4. En la lista de tipo de servicio, seleccione la aplicación o el servicio que desea permitir o bloquear. La lista ya muestra varios servicios comunes, pero no solo dispone de esas opciones. Para añadir cualquier otro servicio o aplicación que no aparezca ya, seleccione **Definido por el usuario**.
5. En Definido por el usuario, seleccione el protocolo e introduzca el nombre y el intervalo de números de puerto del servicio. Si se trata de servicios conocidos, los campos se rellenarán automáticamente.

   Si sabe que la aplicación utiliza TCP o UDP, seleccione el protocolo pertinente. Si no está seguro, seleccione **TCP/UDP**.
6. Introduzca los números de puerto de inicio y de destino. Si la aplicación utiliza un solo número de puerto, introduzca ese número en ambos campos.
7. Introduzca la dirección IP del equipo que desee bloquear.
8. Haga clic en **Añadir** para activar las opciones seleccionadas en Configuración de bloqueo de servicios.

Notificaciones por correo electrónico de eventos de seguridad

Para recibir registros y alertas por correo electrónico, facilite la información de su correo electrónico en la pantalla Correo electrónico y especifique qué alertas desea recibir y con qué frecuencia.

➢ **Para configurar las notificaciones por correo electrónico:**

1. Seleccione **Avanzado > Seguridad > Correo electrónico** para acceder a la siguiente pantalla:



2. Para recibir registros y alertas por correo electrónico de la puerta de enlace, active la casilla **Activar la notificación por correo electrónico**.
3. En el campo Su servidor de correo saliente, introduzca el nombre del servidor de correo saliente (SMTP) de su ISP (por ejemplo, mail.myISP.com). Podrá encontrar esta información en la pantalla de configuración de su programa de correo electrónico. Si este campo está en blanco, no se enviará ningún mensaje de alerta ni registro.
4. Introduzca la dirección de correo electrónico a la que se enviarán los registros y las alertas en el campo Enviar a esta dirección de correo electrónico. También se utilizará esta dirección de correo electrónico como dirección del remitente. Si este campo está en blanco, no se enviará ningún mensaje de alerta ni registro.
5. Si el servidor de correo electrónico saliente requiere autenticación, seleccione la casilla **Mi servidor de correo requiere autenticación**. Rellene los campos Nombre de usuario y Contraseña del servidor de correo saliente.

Después de enviar el registro, este se eliminará de la memoria de la puerta de enlace. Si la puerta de enlace no puede enviar por correo electrónico el archivo de registro, se llenará el búfer de registros. En tal caso, la puerta de enlace sobrescribirá el registro y bloqueará su contenido.

Haga clic en **Aplicar** para guardar la configuración.

Administración

Administración de la red

5

Este capítulo describe la configuración de la puerta de enlace para administrar y mantener la puerta de enlace y la red doméstica.

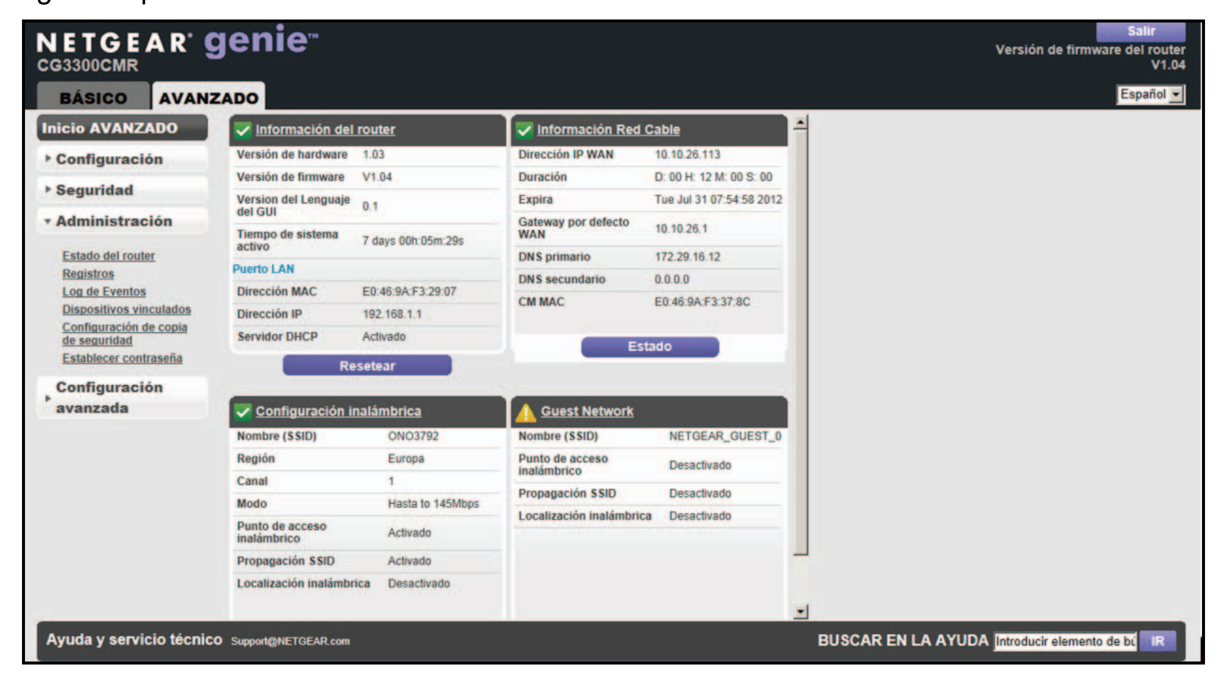
Este capítulo contiene las siguientes secciones:

- *Ver el estado de la puerta de enlace*
- *Ver los registros de acceso web o de intento de acceso web*
- *Ver los logs de eventos*
- *Gestionar el archivo de configuración*
- *Establecer contraseña*

Ver el estado de la puerta de enlace

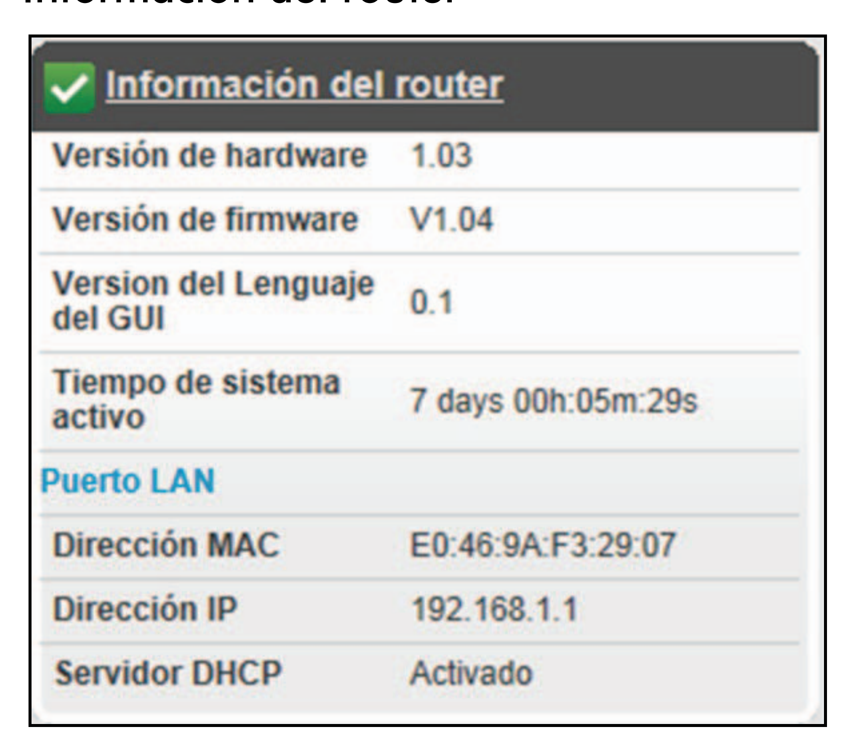
➢ **Para ver los datos de uso y estado de la puerta de enlace:**

Seleccione **Inicio Avanzado** o seleccione **Administración > Estado del router** para ver la siguiente pantalla:



Para acceder a una descripción del elemento del menú Dispositivos vinculados, consulte *Dispositivos vinculados* en la página 19.

Información del router



Aparecerán los siguientes parámetros:

Versión de hardware. El modelo de la puerta de enlace.

Versión de firmware. La versión del firmware de la puerta de enlace. Cambiará cuando se actualice el firmware de la puerta de enlace.

Versión del lenguaje del GUI. El idioma localizado de la interfaz de usuario.

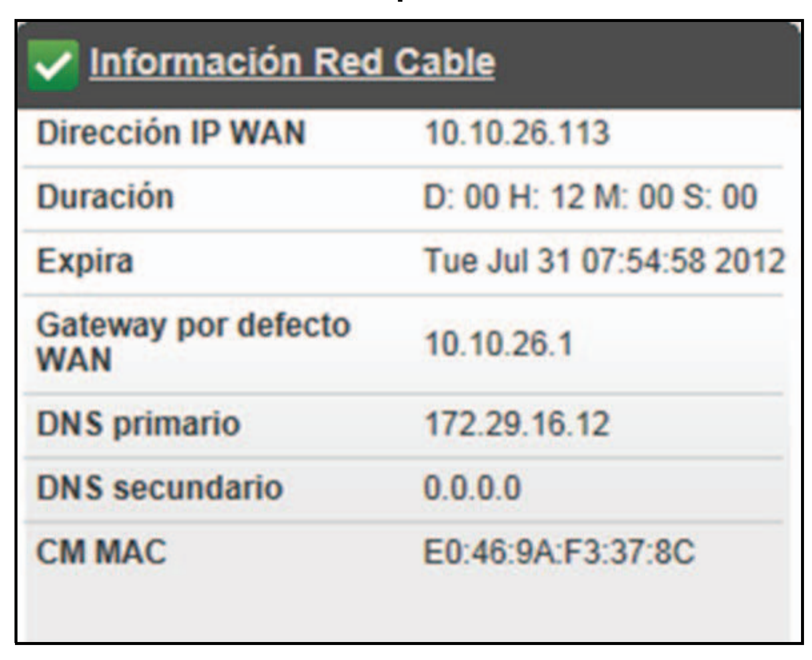
Tiempo de sistema activo. El tiempo que lleva funcionando el sistema.

Puerto LAN.

- **Dirección MAC**. La dirección Media Access Control. Esta dirección es la dirección física única que utiliza el puerto Ethernet (LAN) de la puerta de enlace.
- **Dirección IP**. La dirección IP que utiliza el puerto Ethernet (LAN) de la puerta de enlace. El valor predeterminado es 192.168.1.1.
- **Servidor DHCP**. Identifica si está activo el servidor DHCP integrado de la puerta de enlace para los dispositivos vinculados a la LAN.

Haga clic en el botón **Resetear** para resetear la puerta de enlace.

Información de red por cable



Información Red Cable	
Dirección IP WAN	10.10.26.113
Duración	D: 00 H: 12 M: 00 S: 00
Expira	Tue Jul 31 07:54:58 2012
Gateway por defecto WAN	10.10.26.1
DNS primario	172.29.16.12
DNS secundario	0.0.0.0
CM MAC	E0:46:9A:F3:37:8C

Aparecerán los siguientes parámetros:

Dirección IP WAN. La dirección IP que utiliza el puerto de Internet (WAN) de la puerta de enlace. Si no aparece ninguna dirección o si la dirección es 0.0.0.0, la puerta de enlace no puede conectarse a Internet.

Duración. El tiempo que lleva funcionando la unidad hasta el momento.

Expira. Hora en la que expira la dirección IP de la WAN.

Máscara de subred WAN. La máscara de subred IP que utiliza el puerto de Internet (WAN) de la puerta de enlace.

Gateway por defecto WAN.

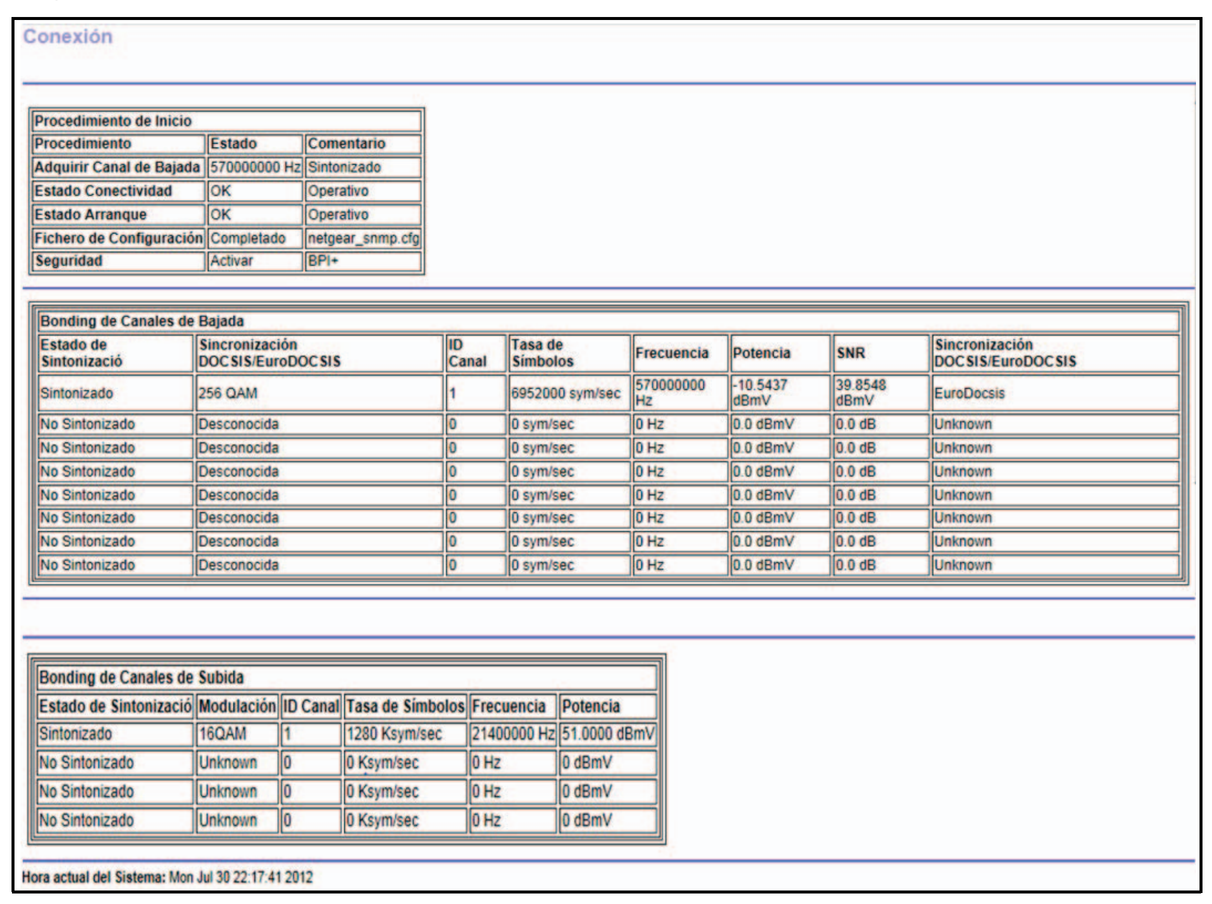
DNS primario. La dirección del servidor de nombres de dominio principal que utiliza la puerta de enlace. Un servidor de nombres de dominio traduce las URL en lenguaje humano, por ejemplo www.netgear.com, a direcciones IP.

DNS secundario. La dirección del servidor de nombres de dominio secundario que utiliza la puerta de enlace.

Estado de la conexión por cable

Para ver el estado de la conexión por cable:

Haga clic en el botón **Estado** para ver la pantalla Conexión por cable.



Conexión

Procedimiento de Inicio		
Procedimiento	Estado	Comentario
Adquirir Canal de Bajada	570000000 Hz	Sintonizado
Estado Conectividad	OK	Operativo
Estado Arranque	OK	Operativo
Fichero de Configuración	Completado	netgear_snmp.cfg
Seguridad	Activar	BPI+

Bonding de Canales de Bajada							
Estado de Sintonizació	Sincronización DOCSIS/EuroDOCSIS	ID Canal	Tasa de Símbolos	Frecuencia	Potencia	SNR	Sincronización DOCSIS/EuroDOCSIS
Sintonizado	256 QAM	1	6952000 sym/sec	570000000 Hz	-10.5437 dBmV	39.8548 dBmV	EuroDocsis
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
No Sintonizado	Desconocida	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown

Bonding de Canales de Subida					
Estado de Sintonizació	Modulación	ID Canal	Tasa de Símbolos	Frecuencia	Potencia
Sintonizado	16QAM	1	1280 Ksym/sec	21400000 Hz	51.0000 dBmV
No Sintonizado	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV
No Sintonizado	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV
No Sintonizado	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV

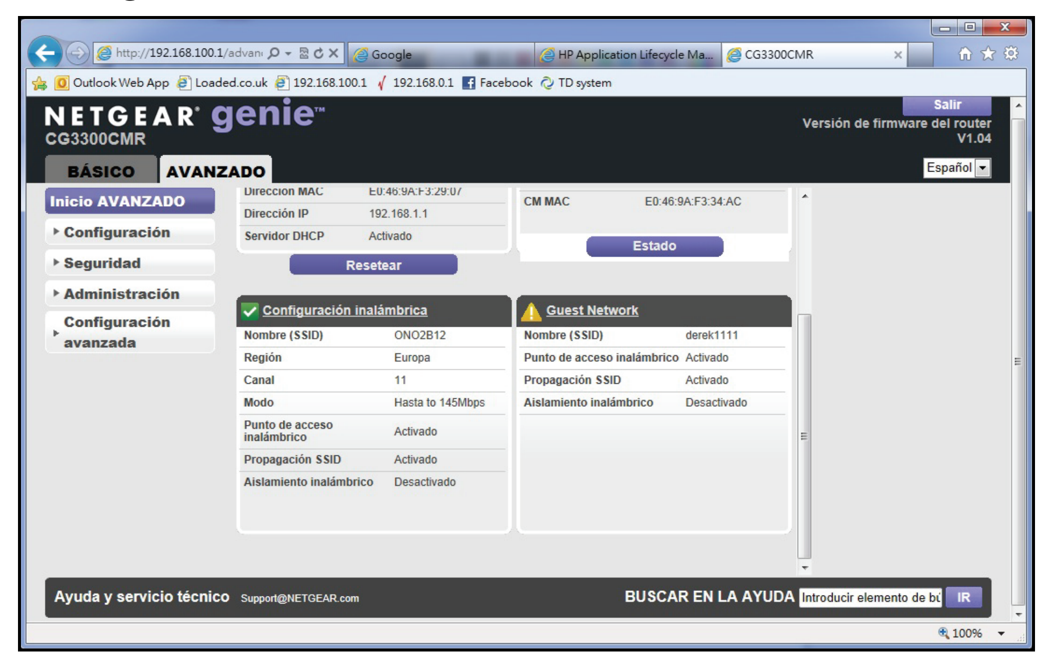
Hora actual del Sistema: Mon Jul 30 22:17:41 2012

Utilice la pantalla Conexión para controlar del proceso de inicialización de la puerta de enlace y para obtener más detalles acerca del canal de cable de los flujos de bajada y de subida. La hora se muestra una vez se ha inicializado la puerta de enlace.

La puerta de enlace lleva a cabo automáticamente los siguientes pasos durante el proceso de aprovisionamiento:

- Busca y bloquea la frecuencia del flujo de bajada y, a continuación, vuelve a alinearla con la dirección del flujo de subida.
- Obtiene una dirección IP para la propia puerta de enlace. A continuación, la puerta de enlace asigna una dirección IP al equipo conectado.
- Se conecta a Internet.

Configuración inalámbrica



Aparecerán los siguientes parámetros:

Nombre (SSID). El nombre de la red inalámbrica (SSID) que utiliza la puerta de enlace.

Región. La zona geográfica en la que se está utilizando la puerta de enlace. En algunas partes del mundo, es ilegal utilizar las funciones inalámbricas de la puerta de enlace.

Canal. Identifica el canal operativo del puerto inalámbrico que se está usando. El canal predeterminado es Auto. Cuando está seleccionada la opción Auto, la puerta de enlace busca el mejor canal operativo disponible. Si experimenta interferencias de dispositivos cercanos, puede seleccionar otro canal. Los canales 1, 6 y 11 no interfieren entre sí.

Modo. Indica el modo de comunicación inalámbrico: hasta 54 Mbps, hasta 145 Mbps (predeterminado) y hasta 300 Mbps.

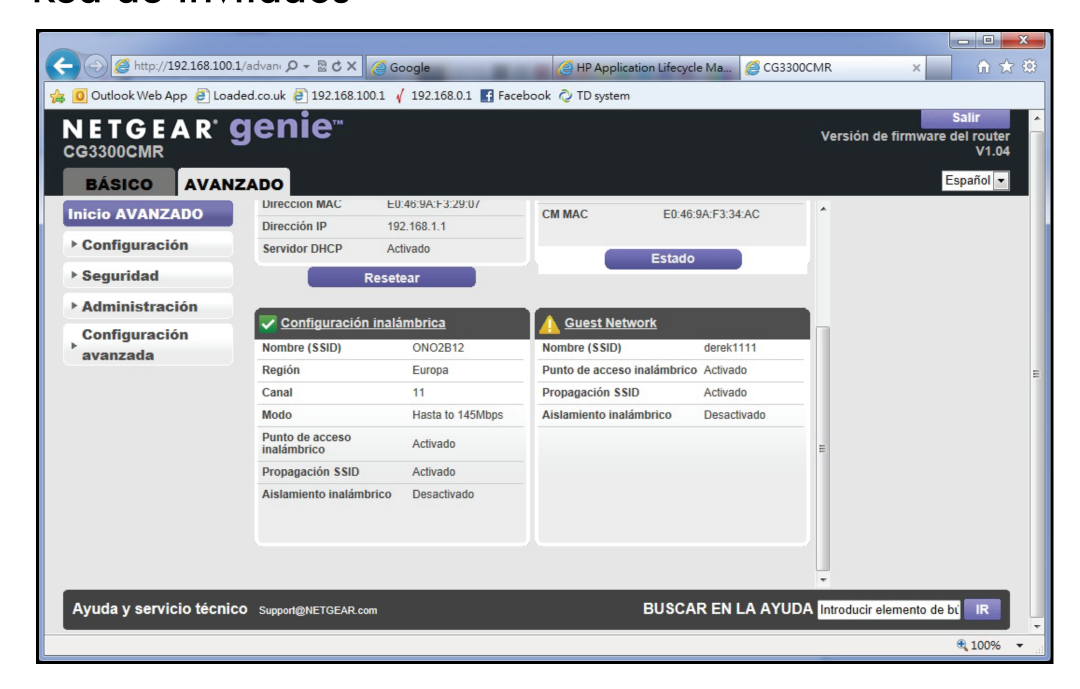
Punto de acceso inalámbrico. Indica si está activada la función de radio de la puerta de enlace. Si no lo está, el indicador de actividad inalámbrica situado en el panel delantero estará apagado.

Propagación SSID. Indica si la puerta de enlace emite el SSID.

Aislamiento Inalámbrico. Indica que los clientes podrán conectarse a Internet. Sin embargo, no podrán tener acceso entre sí ni tampoco a cualquier dispositivo de la red.

Wi-Fi Protected Setup. Indica si se ha configurado Wi-Fi Protected Setup para la red.

Red de invitados



Aparecerán los siguientes parámetros:

Nombre (SSID). El nombre (SSID) de la red inalámbrica 11N que utiliza la puerta de enlace. El nombre predeterminado es NETGEAR_Guest_0.

Punto de acceso inalámbrico. Indica si está activada la función de radio de la puerta de enlace. Si no lo está, los indicadores de actividad inalámbrica situados en el panel delantero estarán apagados.

Propagación SSID. Indica si la puerta de enlace emite el SSID.

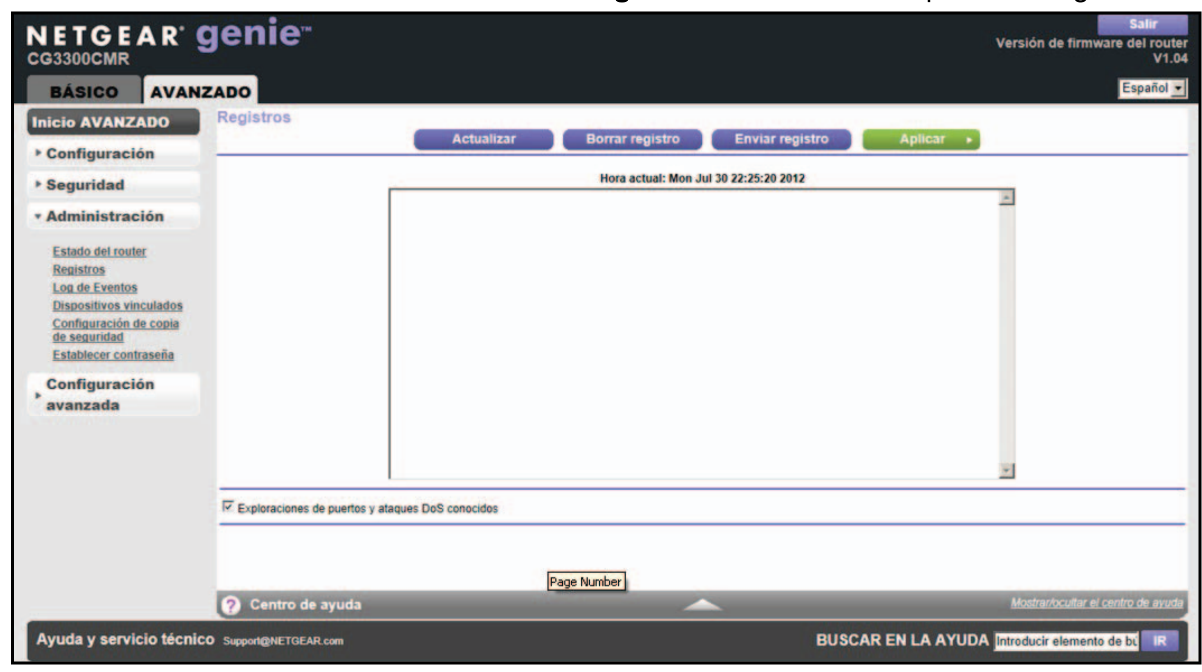
Aislamiento inalámbrico. Indica que se permite la conexión inalámbrica a la puerta de enlace.

Ver los registros de acceso web o de intento de acceso web

El registro es un informe pormenorizado de los sitios web a los que ha accedido o tratado de acceder. En él, se guardan hasta 256 entradas. Las entradas del registro solo aparecen si se ha activado el bloqueo de palabras clave y no se realiza ninguna entrada en el registro respecto al cliente LAN seguro.

➢ **Para ver los registros:**

Seleccione **Avanzado > Administración > Registros**. Se mostrará la pantalla Registros.



La pantalla de registros muestra la siguiente información:

- **Fecha y hora**. La fecha y la hora en las que se registró la entrada.
- **IP de origen**. La dirección IP del dispositivo que inició esta entrada.
- **Dirección de destino**. El nombre o la dirección IP del sitio web o el grupo de noticias visitado o al que se ha tratado de acceder.
- **Acción**. Si se permitió o se bloqueó el acceso.
- **Exploraciones de puertos y ataques DoS conocidos**. Desactive esta casilla para ignorar exploraciones de puertos y ataques DoS conocidos.

Para actualizar la pantalla de registros, haga clic en el botón **Actualizar**.

Para eliminar las entradas de registro, haga clic en el botón **Borrar registro**.

Para enviar por correo el registro de inmediato, haga clic en el botón **Enviar registro**.

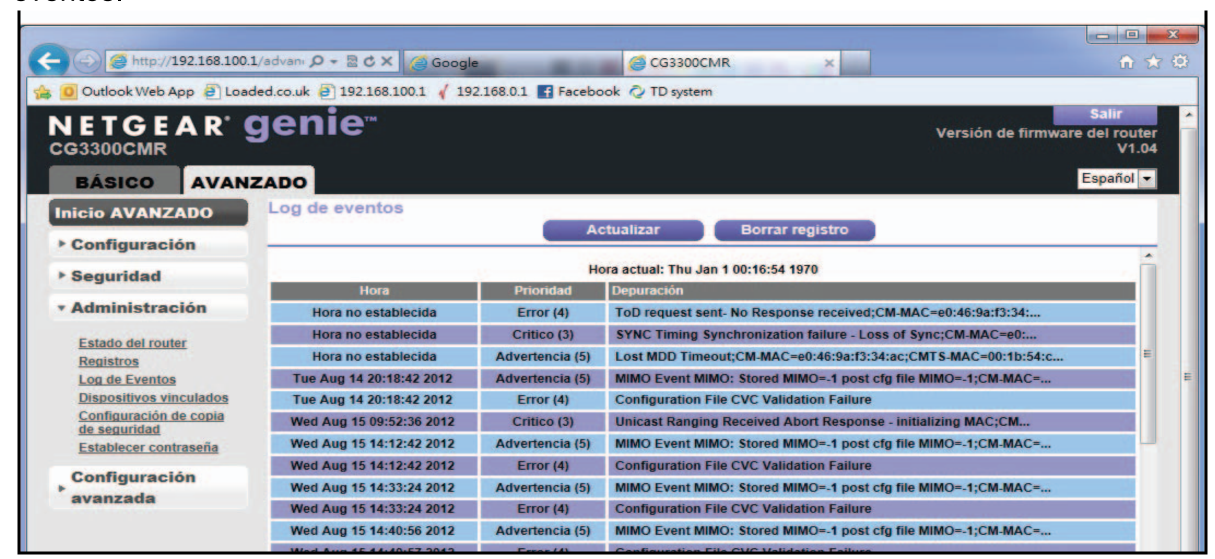
Para guardar los cambios, haga clic en el botón **Aplicar**.

Ver los logs de eventos

Los logs de eventos capturan eventos importantes de la puerta de enlace.

➤ **Para ver los logs de eventos:**

Seleccione **Avanzado > Administración > Log de eventos**. Se mostrará la pantalla Log de eventos.



La pantalla de registros muestra la siguiente información:

- **Hora**. La hora a la que se registró la entrada del log de eventos.
- **Prioridad**. La importancia de esta entrada del log de eventos.
- **Descripción**. Una descripción de esta entrada del log de eventos.

Para actualizar la pantalla de registros, haga clic en el botón **Actualizar**.

Para eliminar las entradas de registro, haga clic en el botón **Borrar registro**.

Gestionar el archivo de configuración

Los ajustes de configuración de la puerta de enlace por cable inalámbrica se guardan dentro de la propia puerta de enlace en un archivo de configuración. Podrá hacer una copia de seguridad (guardar) de este archivo en su equipo, o restablecerlo con la configuración predeterminada de fábrica.

Configuración de copia de seguridad

➢ **Para hacer una copia de seguridad de los ajustes de configuración de la puerta de enlace:**

1. Seleccione **Avanzado > Administración > Configuración de copia de seguridad** para acceder a la siguiente pantalla:



2. Haga clic en **Copia de seguridad** para guardar una copia de la configuración actual.
3. Seleccione una ubicación para guardar el archivo .cfg que se encuentre en un equipo de su red.

Restaurar los ajustes de configuración

➢ **Para restaurar los ajustes de configuración de los que haya hecho una copia de seguridad:**

1. Introduzca la ruta completa al archivo en la red o haga clic en el botón **Abrir fichero** para buscar el archivo.
2. Cuando haya localizado el archivo .cfg, haga clic en el botón **Restaurar** para cargar el archivo en la puerta de enlace.

Cuando haya terminado, la puerta de enlace se reinicia.



ADVERTENCIA:

No interrumpa el proceso de reinicio.

Borrar

En determinadas circunstancias (por ejemplo, si mueve la puerta de enlace a una red diferente o si ha olvidado la contraseña), querrá borrar la configuración y restaurar la configuración predeterminada de fábrica.

Pulse el botón **Restaurar configuración de fábrica** de la parte de atrás de la puerta de enlace (consulte *Configuración predeterminada de fábrica* en la página 78) o haga clic en el botón **Borrar** de esta pantalla.

Al borrar, el nombre de usuario pasa a ser admin, la contraseña pasa a ser password y la dirección IP de la LAN pasa a ser 192.168.1.1, y se activa el DHCP de la puerta de enlace.

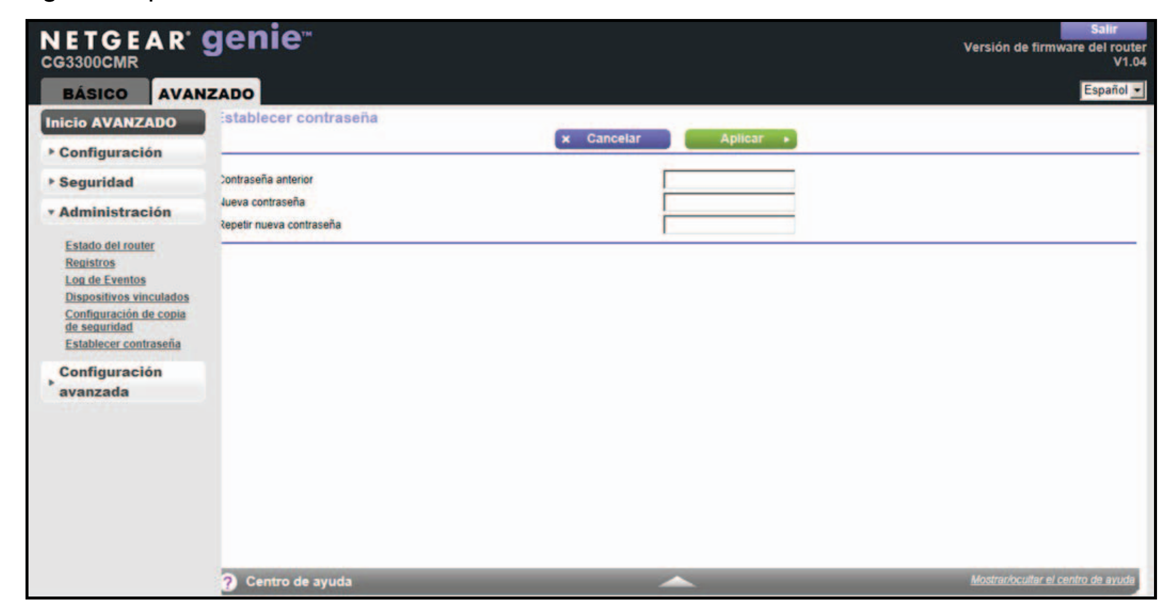
Establecer contraseña

Esta función le permite modificar la contraseña predeterminada que se utiliza para acceder a la puerta de enlace con el nombre de usuario **admin**.

Esta contraseña de la puerta de enlace no es la misma que la contraseña de acceso inalámbrico. La etiqueta de la parte inferior de la puerta de enlace muestra el nombre único de la red inalámbrica (SSID) y la contraseña de acceso inalámbrico (consulte *Etiqueta de la puerta de enlace* en la página 10).

➢ **Para establecer la contraseña del nombre de usuario admin:**

1. Seleccione **Avanzado > Administración > Establecer contraseña** para acceder a la siguiente pantalla:



2. Teclee la contraseña anterior y escriba dos veces la nueva contraseña en los campos de esta pantalla.
3. Haga clic en **Aplicar** para que los cambios surtan efecto.

Configuración avanzada

Ajuste de la red

6

En este capítulo, se describen las funciones avanzadas de la puerta de enlace. Esta información exige un sólido conocimiento de los conceptos sobre redes y está destinada al personal que desee configurar la puerta de enlace para situaciones excepcionales, como por ejemplo, cuando se necesita acceso remoto a través de Internet mediante IP o mediante un nombre de dominio.

Este capítulo contiene las siguientes secciones:

- *Configuración inalámbrica avanzada*
- *Servicios*
- *Reenvío de puertos y Activación de puertos*
- *Configuración de reenvío de puertos a servidores locales*
- *Configurar la activación de puertos*
- *DNS dinámico*
- *Estado del cable*
- *Universal Plug and Play*
- *IPv6*
- *NAT*

Configuración inalámbrica avanzada

➢ **Para ver la configuración inalámbrica avanzada:**

Seleccione **Avanzado > Configuración avanzada > Configuración inalámbrica avanzada** para acceder a la siguiente pantalla:



Configuración inalámbrica avanzada

En esta parte de la pantalla, se encuentran disponibles los parámetros siguientes:

- **Activar radio del router inalámbrico**. Puede apagar por completo la parte inalámbrica de la puerta de enlace inalámbrica si desactiva esta casilla de verificación. Para volver a activar la parte inalámbrica de la puerta de enlace, active de nuevo esta casilla de verificación. Cuando la radio inalámbrica esté desactivada, otros miembros de la familia podrán utilizar la puerta de enlace conectando sus equipos a la puerta de enlace mediante un cable Ethernet.
- **Activar el aislamiento inalámbrico**. Si se ha activado esta casilla de verificación, podrán utilizar Internet los clientes inalámbricos (equipos o dispositivo inalámbricos) que se unan a la red. Sin embargo, no podrán acceder entre sí ni tampoco a los dispositivos Ethernet de la red.
- **Activar emisión de la SSID**. Este parámetro activa la emisión de la SSID.

- **Conectar la configuración WMM (Wi-Fi multimedia).** WMM (Wireless Multimedia) es un conjunto perteneciente al estándar 802.11e. WMM permite que el tráfico inalámbrico disponga de un amplio abanico de prioridades, dependiendo del tipo de los datos. La información cuya distribución inmediata es esencial, como los archivos de audio o vídeo, tienen una mayor prioridad que el tráfico normal. Para que la opción WMM funcione correctamente, los clientes inalámbricos también deben ser compatibles.

Nota: Las opciones Longitud de fragmentación, Umbral CTS/RTS y Modo de preámbulo están reservadas exclusivamente para la configuración avanzada y las pruebas inalámbricas. No se recomienda modificarlas.

- **Control de la potencia de transmisión**. Con la configuración predeterminada de 100%, la puerta de enlace utiliza el nivel de potencia que recomienda la NETGEAR para la transmisión de paquetes inalámbricos. Si modifica este parámetro y establece un porcentaje inferior, ahorrará energía pero también reducirá la cobertura inalámbrica.

Lista de acceso por tarjeta inalámbrica

De forma predeterminada, cualquier equipo o dispositivo inalámbrico configurado con la SSID correcta, dispondrá de acceso a la red inalámbrica. Para mayor seguridad, permita el acceso a la red inalámbrica únicamente a dispositivos y equipos inalámbricos específicos basándose en sus direcciones MAC.

➤ **Para activar el acceso a la tarjeta inalámbrica:**

1. Haga clic en el botón **Configurar lista** para mostrar la pantalla Lista de acceso por tarjeta inalámbrica.



En esta pantalla, es posible restringir el acceso a la red para que solo puedan conectarse dispositivos específicos en función de sus direcciones MAC.

2. Marque la casilla **Activar el control de acceso** para activar la restricción de dispositivos y equipos con conexión inalámbrica según sus direcciones MAC.

Nota: Si la opción Activar el control de acceso está habilitada y Lista de control de accesos está vacía, ningún dispositivo ni equipo inalámbrico podrá conectarse a la red.

---

3. Para obtener información sobre cómo añadir dispositivos y equipos inalámbricos a la Lista de control de accesos, consulte *Configuración de la lista de acceso a clientes inalámbricos* en la página 55.
4. Haga clic en el botón **Aplicar** para guardar los cambios y regresar a la pantalla Configuración inalámbrica avanzada.

Configuración de la lista de acceso a clientes inalámbricos

➢ **Para configurar la lista de control de accesos:**

1. Haga clic en el botón **Añadir** de la pantalla Lista de acceso por tarjeta inalámbrica para acceder a la pantalla de configuración de la lista de acceso por tarjeta inalámbrica.

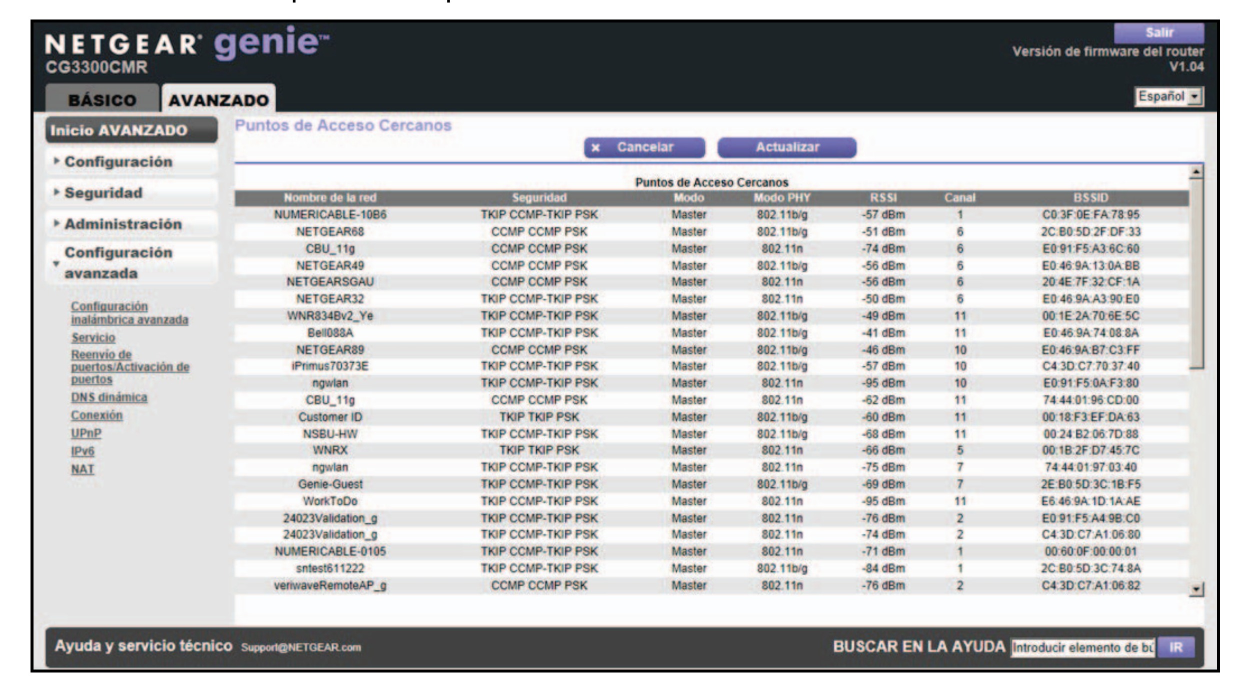


Esta pantalla incluye una lista de dispositivos y equipos inalámbricos activos actualmente y sus direcciones MAC Ethernet.

2. Si el dispositivo o el equipo inalámbrico que desea aparece en la lista, haga clic en el botón de opción correspondiente para capturar su dirección MAC. De no ser así, introduzca manualmente la dirección MAC del dispositivo o equipo inalámbrico autorizado. La dirección MAC se encuentra en el equipo o en el dispositivo.
3. Si no aparece ningún nombre de dispositivo, escriba un nombre descriptivo para el equipo o el dispositivo que está añadiendo.
4. Cuando haya acabado de introducir la dirección MAC, haga clic en el botón **Añadir** para regresar a la pantalla Lista de acceso inalámbrico.
5. Repita los pasos 1 a 4 para cada uno de los dispositivos o equipos inalámbricos.
6. Cuando haya terminado de añadir dispositivos y equipos inalámbricos a esta lista, en la pantalla de configuración de la lista de acceso por tarjeta inalámbrica, active la casilla de verificación **Activar el control de acceso** para habilitar el control de acceso.
7. En la pantalla de configuración de la lista de acceso por tarjeta inalámbrica, haga clic en **Aplicar** para guardar los cambios y volver a la pantalla Configuración inalámbrica avanzada.

Puntos de acceso cercanos

Haga clic en el botón **Buscar puntos de acceso** para encontrar puntos de acceso cercanos a la CG3300CMR. Aparecerá la pantalla Puntos de acceso cercanos.



Servicios

➢ **Para ver la configuración inalámbrica avanzada:**

Seleccione **Avanzado > Configuración avanzada > Servicios** para acceder a la siguiente pantalla:



Utilice la pantalla Servicios para desactivar determinadas funciones de la puerta de enlace. Para deshabilitar una función, desactive la casilla correspondiente.

- Si se ha activado Características del firewall, la puerta de enlace lleva a cabo la inspección dinámica de paquetes (SPI) y protege frente a los ataques de denegación de servicio (DoS).
- Si está activado IPSec Pass-Through, se reenviará el tráfico IPSec. Si está desactivada esta función, este tráfico se bloquea.
- Si está activado PPTP Pass-Through, se reenviará el tráfico PPTP. Si está desactivada esta función, este tráfico se bloquea.
- Si está activado Multicast, la puerta de enlace por cable realiza las transmisiones de emisión múltiple a través del firewall.
- Si está activado Detección de escaneo de puertos, la puerta de enlace por cable responderá a los escaneos de puerto basados en Internet.
- Si está activado Detección IP Flood, la puerta de enlace por cable bloqueará los dispositivos malintencionados que intenten atacar los dispositivos.

Utilice Funcionalidades Web para que el firewall bloquee determinadas cookies de navegadores web, secuencias de comandos de Java y ventanas emergentes.

Haga clic en el botón **Aplicar** para guardar la configuración.

Reenvío de puertos y Activación de puertos

De forma predeterminada, la puerta de enlace bloque el tráfico de entrada de Internet a los equipos, salvo las respuestas al tráfico de salida. Para los siguientes fines, cree excepciones a esta norma:

- Permitir que equipos remotos en Internet accedan a un servidor de su red local.
- Permitir que determinadas aplicaciones y juegos funcionen correctamente cuando la puerta de enlace no reconozca sus respuestas.

La puerta de enlace dispone de dos funciones para crear estas excepciones: reenvío de puertos y activación de puertos. En los siguientes apartados, se ofrece información general para que comprenda cómo funcionan y las diferencias que existen entre ambas.

Aspectos básicos sobre el acceso de equipos remotos

Cuando un equipo de su red acceda a otro en Internet, su equipo enviará a la puerta de enlace un mensaje con la dirección de origen y destino, y con información de proceso. Antes de reenviar el mensaje al equipo remoto, la puerta de enlace tiene que modificar la información de origen, crear una sesión de comunicación y hacer un seguimiento de esta de manera que se puedan volver a enrutar las respuestas hacia su equipo.

A continuación, le mostramos un ejemplo de tráfico de salida normal y de las respuestas de entrada resultantes:

1. Se abre un navegador y el sistema operativo asigna el número de puerto 5678 a esta sesión del navegador.
2. Se teclea http://www.example.com en el campo de la URL y el ordenador crea un mensaje de solicitud de página web con la siguiente información de puerto y dirección. Se envía el mensaje de solicitud a la puerta de enlace.

   Dirección de origen. La dirección IP del equipo.

   Número de puerto de origen. 5678, que es la sesión del navegador.

   Dirección de destino. La dirección IP de www.example.com, que su equipo averigua preguntando a un servidor DNS.

   Número de puerto de destino. 80, que es el número de puerto estándar de un proceso de servidor web.

3. La puerta de enlace creará una entrada en su tabla de sesiones internas con la descripción de esta sesión de comunicación entre su equipo y el servidor web en www.example.com. Antes de enviar la solicitud de página web a www.example.com, la puerta de enlace almacenará la información original y, a continuación, modificará la información de origen del mensaje de solicitud, realizando una traducción de direcciones de red (NAT):
   - La dirección de origen se sustituye por la dirección IP pública de la puerta de enlace. Este paso es necesario porque el equipo utiliza una dirección IP privada que no es única en el mundo, por lo que no se puede utilizar en Internet.

- Se cambia el número de puerto de origen por un número elegido por la puerta de enlace, por ejemplo, 33333. Este paso es necesario porque dos equipos podrían estar utilizando el mismo número de sesión de forma independiente.

A continuación, la puerta de enlace envía este mensaje de solicitud al servidor web de www.example.com a través de Internet.

4. El servidor web de www.example.com redacta un mensaje de respuesta con los datos de la página web solicitada. El mensaje devuelto incluirá la siguiente información sobre el puerto y la dirección. A continuación, el servidor web enviará este mensaje de respuesta a la puerta de enlace.

   Dirección de origen. La dirección IP de www.example.com.

   Número de puerto de origen. 80, que es el número de puerto estándar de un proceso de servidor web.

   Dirección de destino. La dirección IP pública de la puerta de enlace.

   Número de puerto de destino. 33333.

5. Tras haber recibido el mensaje entrante, la puerta de enlace comprobará la tabla de sesiones para establecer si hay alguna sesión activa con el número de puerto 33333. Al buscar una sesión activa, la puerta de enlace modificará el mensaje para restaurar la información de dirección original sustituida por la NAT. La puerta de enlace enviará este mensaje de respuesta a su equipo, que mostrará la página web de www.example.com. El mensaje devuelto incluirá entonces la siguiente información sobre el puerto y la dirección.

   Dirección de origen. La dirección IP de www.example.com.

   Número de puerto de origen. 80, que es el número de puerto estándar de un proceso de servidor web.

   Dirección de destino. La dirección IP del equipo.

   Número de puerto de destino. 5678, que es la sesión del navegador que realizó la solicitud inicial.

6. Cuando finalice la sesión del navegador, la puerta de enlace detectará finalmente un periodo de inactividad en las comunicaciones. Entonces, la puerta de enlace eliminará la información de la sesión de su tabla de sesiones y ya no se aceptará tráfico entrante en el número de puerto 33333.

Activación de puertos para puertos de entrada abiertos

En el ejemplo anterior, la puerta de enlace envía las solicitudes a un equipo remoto desde un número de puerto del servicio concreto y las respuestas del equipo remoto a la puerta de enlace se dirigen a ese número de puerto. Si el servidor remoto envía una respuesta a un número de puerto diferente, la puerta de enlace no la reconocerá y la bloqueará. Si embargo, algunos servidores de aplicaciones (por ejemplo, servidores FTP e IRC) envían respuestas a varios números de puerto. Mediante la función de activación de puertos de la puerta de enlace, podrá indicarle a la puerta de enlace que abra otros puertos de entrada cuando una sesión se origine en un puerto de salida concreto.

Un ejemplo de esto es Internet Relay Chat (IRC). Su equipo se conecta a un servidor IRC en el puerto de destino 6667. El servidor IRC no solo responde a su puerto de origen, sino que también enviará un mensaje de “identificación” a su equipo en el puerto 113. Mediante la activación de puertos, podrá indicar a la puerta de enlace, “Cuando se inicie una sesión con puerto de destino 6667, también tendrás que permitir que el tráfico entrante del puerto 113 llegue al equipo de origen”. Utilizando pasos similares al ejemplo anterior, la siguiente secuencia muestra los efectos de la norma de activación de puertos que ha definido:

1. Se abre un programa cliente de IRC para iniciar una sesión de chat en el equipo.
2. El cliente IRC escribe un mensaje de solicitud a un servidor IRC utilizando el número de puerto de destino 6667, el número de puerto estándar de un proceso de servidor IRC. A continuación, el equipo enviará este mensaje de solicitud a la puerta de enlace.
3. La puerta de enlace creará una entrada en su tabla de sesiones internas con la descripción de esta sesión de comunicación entre su equipo y el servidor IRC. La puerta de enlace almacenará la información original, realizará la traducción de direcciones de red (NAT) en el puerto y la dirección de origen, y enviará este mensaje de solicitud por Internet al servidor IRC.
4. Teniendo en cuenta la norma de activación de puertos y tras haber observado el número de puerto de destino 6667, la puerta de enlace creará otra entrada de sesión para enviar cualquier tráfico del puerto de entrada 113 a su equipo.
5. El servidor IRC enviará un mensaje de respuesta a la puerta de enlace utilizando un puerto de origen asignado por la NAT (al igual que en el ejemplo anterior, por ejemplo, el puerto 33333) como puerto de destino. El servidor IRC envía también un mensaje de identificación a la puerta de enlace con el puerto de destino 113.
6. Tras haber recibido el mensaje entrante para el puerto de destino 33333, la puerta de enlace comprobará la tabla de sesiones para establecer si hay alguna sesión activa en el número de puerto 33333. Tras encontrar una sesión activa, la puerta de enlace restaurará la información de la dirección original sustituida por la NAT y enviará el mensaje de respuesta a su equipo.
7. Tras haber recibido el mensaje entrante para el puerto de destino 113, la puerta de enlace comprobará la tabla de sesiones y verá que hay una sesión activa con el número de puerto 113 asociada a su equipo. La puerta de enlace cambiará la dirección IP de destino del mensaje por la dirección IP del equipo y enviará el mensaje a su equipo.
8. Cuando finalice la sesión de chat, la puerta de enlace detectará finalmente un periodo de inactividad en las comunicaciones. Entonces, la puerta de enlace eliminará la información de la sesión de su tabla de sesiones y ya no se aceptará tráfico entrante en los puertos 33333 ni 113.

Para configurar la activación de puertos, tiene que saber qué puertos de entrada necesita la aplicación. Además, tiene que conocer el número del puerto de salida que activa la apertura de los puertos de entrada. Normalmente, para conocer dicha información, podrá ponerse en contacto con el autor de la aplicación, o bien con grupos de usuarios o grupos de noticias de la misma.

Nota: La aplicación que ha provocado la activación de puertos no podrán utilizarla varios equipos al mismo tiempo.

Reenvío de puertos para permitir comunicaciones de host externas

En los dos ejemplos anteriores, el equipo inicia una sesión de la aplicación con un equipo del servidor en Internet. Sin embargo, debe permitir que un equipo cliente en Internet inicie una conexión con un equipo del servidor en la red. Por lo general, la puerta de enlace ignora cualquier tráfico de entrada que no sea una respuesta a su propio tráfico de salida. Puede configurar excepciones a esta norma predeterminada utilizando la función de reenvío de puertos.

Se puede mostrar una aplicación habitual del reenvío de puertos invirtiendo la relación entre cliente y servidor del ejemplo anterior del servidor web. En este caso, un navegador de un equipo remoto accede a un servidor web que se ejecuta en un ordenador de la red local. Utilizando el reenvío de puertos, podrá indicarle a la puerta de enlace: “Cuando se reciba tráfico entrante en el puerto 80 (el número de puerto estándar de un proceso de servidor web), enrútalo al equipo local en 192.168.1.123”. La siguiente secuencia muestra los efectos de la norma de reenvío de puertos que ha definido:

1. El usuario de un equipo remoto abre un navegador y solicita una página web de www.example.com, que se resuelve con la dirección IP pública de la puerta de enlace. El equipo remoto escribe un mensaje de solicitud de página web con la siguiente información de destino:

   Dirección de destino. La dirección IP de www.example.com, que es la dirección de la puerta de enlace.

   Número de puerto de destino. 80, que es el número de puerto estándar de un proceso de servidor web.

   Después, el equipo remoto envía este mensaje de solicitud por Internet a la puerta de enlace.

2. La puerta de enlace recibe el mensaje de solicitud y analiza su tabla de normas por si hubiera alguna sobre el bloqueo del tráfico del puerto de entrada 80. La norma de reenvío de puertos especifica que se enrute el tráfico del puerto de entrada 80 a la dirección IP local 192.168.1.123. Por lo tanto, la puerta de enlace modifica la información de destino del mensaje de solicitud:

   La dirección de destino se sustituye por 192.168.1.123.

   A continuación, la puerta de enlace envía este mensaje de solicitud a la red local.

3. El servidor web de 192.168.1.123 recibe la solicitud y redacta un mensaje de respuesta con los datos de la página web solicitada. A continuación, el servidor web envía este mensaje de respuesta a la puerta de enlace.

4. La puerta de enlace realiza la traducción de direcciones de red (NAT) de la dirección IP de origen y envía el mensaje de solicitud por Internet al equipo remoto, el cual visualiza la página web de www.example.com.

Para configurar el reenvío de puertos, tiene que saber qué puertos de entrada necesita la aplicación. Normalmente, para conocer dicha información, podrá ponerse en contacto con el autor de la aplicación, o bien con grupos de usuarios y grupos de noticias pertinentes.

Diferencias entre el reenvío de puertos y la activación de puertos

En los puntos siguientes, se resumen las diferencias entre el reenvío de puertos y la activación de puertos:

- La activación de puertos es utilizada por cualquier equipo de la red, aunque solo podrá utilizarla un equipo cada vez.
- El reenvío de puertos se configura para un solo equipo de la red.
- La activación de puertos exige que tráfico de salida concreto abra los puertos de entrada y los puertos activados se cierren tras un periodo de inactividad.
- El reenvío de puertos siempre está activo.

Configuración de reenvío de puertos a servidores locales

Utilizando la función de reenvío de puertos, puede permitir que algunos tipos de tráfico entrante lleguen a servidores de su red local. Por ejemplo, quiere que un servidor web, servidor FTP o servidor de juegos local pueda verse y esté disponible por Internet.

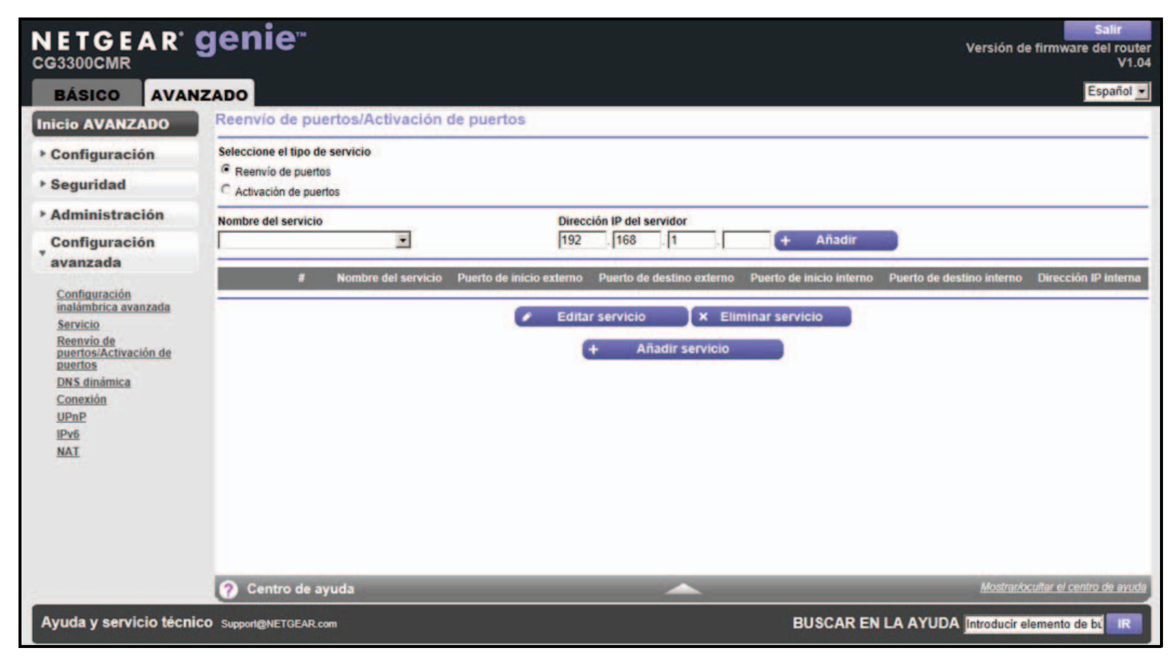
Utilice la pantalla Reenvío de puertos/Activación de puertos para configurar la puerta de enlace para dirigir protocolos entrantes concretos a equipos de la red local. Además de los servidores de aplicaciones específicas, también puede especificar un servidor DMZ predeterminado al que se envíen todos los demás protocolos entrantes.

Antes de comenzar, determine qué tipo de servicio, aplicación o juego quiere ofrecer, y la dirección IP local del equipo que ofrece el servicio. El equipo del servidor siempre debe tener la misma dirección IP.

➤ **Para configurar el reenvío de puertos:**

Consejo: Para asegurarse de que el equipo del servidor tenga siempre la misma dirección IP, utilice la función de dirección IP reservada de la puerta de enlace.

1. Seleccione **Configuración avanzada > Reenvío de puertos/Activación de puertos** para acceder a la siguiente pantalla:



Se seleccionará Reenvío de puertos como tipo de servicio.

2. En la lista Nombre del servicio, seleccione el servicio o el juego que aloja en la red. Si dicho servicio no aparece en la lista, consulte *Añadir un servicio personalizado* en la página 63.
3. En el campo Dirección IP del servidor correspondiente, introduzca el último dígito de la dirección IP del equipo local que ofrezca este servicio.
4. Haga clic en **Añadir**. El servicio aparecerá en la lista de la pantalla.

Añadir un servicio personalizado

Para definir un servicio, juego o aplicación que no aparezca en la lista Nombre del servicio, establezca el número de puerto o el intervalo de números que utiliza la aplicación. Normalmente, para conocer dicha información, podrá ponerse en contacto con el autor de la aplicación, o bien con grupos de usuarios o grupos de noticias de la misma.

➤ **Para añadir un servicio personalizado:**

1. Seleccione **Avanzado > Configuración avanzada > Reenvío de puertos/Activación de puertos**.
2. Seleccione **Reenvío de puertos** como tipo de servicio.

3. Haga clic en el botón **Añadir servicio** para acceder a la siguiente pantalla:



4. En el campo Nombre del servicio, introduzca un nombre descriptivo.
5. En la lista Protocolo, seleccione el protocolo. Si no está seguro, seleccione **TCP/UDP**.
6. En los campos de puerto de inicio, introduzca el número de puerto de inicio.
   - Si la aplicación utiliza un solo puerto, escriba el número de dicho puerto en el campo Puerto de destino.
   - Si la aplicación utiliza varios puertos, escriba el último número de puerto del intervalo en el campo Puerto de destino.
7. En el campo Dirección IP interna, introduzca la dirección IP del equipo local que ofrece este servicio.
8. Haga clic en **Aplicar**. El servicio aparecerá en la lista de la pantalla Reenvío de puertos/Activación de puertos.

Editar o eliminar una entrada de reenvío de puertos

➤ **Para editar o eliminar una entrada de reenvío de puertos:**

1. En la tabla, seleccione el botón de opción que está al lado del nombre del servicio.
2. Haga clic en **Editar servicio** o **Eliminar servicio**.

Ejemplo de aplicación: convertir en público un servidor web local

Si aloja un servidor web en la red local, podrá utilizar el reenvío de puertos para permitir que lleguen al servidor web las solicitudes web de cualquier persona en Internet.

➢ **Para convertir en público un servidor web local:**

1. Asigne al servidor web una dirección IP fija o una dirección IP dinámica mediante la reserva de direcciones DHCP. En este ejemplo, la puerta de enlace asigna siempre al servidor web la dirección IP 192.168.1.33.
2. En la pantalla Reenvío de puertos/Activación de puertos, configure la puerta de enlace para reenviar el servicio HTTP a la dirección local del servidor web de **192.168.1.33**. HTTP (puerto 80) es el protocolo estándar de los servidores web.
3. (Opcional) Registre un nombre de host con un servicio DNS dinámico y configure la puerta de enlace para que utilice el nombre descrito en *DNS dinámico* en la página 67. Para acceder al servidor web por Internet, un usuario remoto deberá conocer la dirección IP que asigna su ISP. Sin embargo, si utiliza un servicio DNS dinámico, el usuario remoto podrá acceder al servidor con un nombre de Internet sencillo, por ejemplo, mynetgear.dyndns.org.

Configurar la activación de puertos

La activación de puertos es una extensión dinámica del reenvío de puertos que resulta útil en los siguientes casos:

- Más de un equipo local precisa el reenvío de puertos para la misma aplicación (pero no de forma simultánea).
- Una aplicación abre puertos de entrada que sean diferentes del puerto de salida.

Si se habilita la activación de puertos, la puerta de enlace controlará el tráfico de salida en busca de un puerto "activado" de salida específico. Si la puerta de enlace detecta tráfico de salida en dicho puerto, recordará la dirección IP del equipo local que envió los datos. A continuación, la puerta de enlace abrirá temporalmente el puerto o los puertos de entrada especificados y reenviará el tráfico entrante de los puertos activados al equipo de activación.

Aunque el reenvío de puertos crea una asignación estática de un intervalo o número de puerto a un solo equipo local, la activación de puertos puede abrir de manera dinámica los puertos a cualquier equipo que lo necesite y puede cerrar los puertos cuando ya no sean necesarios.

Nota: Si utiliza aplicaciones como los juegos multijugador, las conexiones peer-to-peer, las comunicaciones en tiempo real como la mensajería instantánea o bien la asistencia remota (una función de Windows XP), active Universal Plug and Play (UPnP) de acuerdo con las instrucciones de *Universal Plug and Play* en la página 69.

Para configurar la activación de puertos, tiene que saber qué puertos de entrada necesita la aplicación. Además, tiene que conocer el número del puerto de salida que activa la apertura de los puertos de entrada. Normalmente, para conocer dicha información, podrá ponerse en contacto con el autor de la aplicación, o bien con grupos de usuarios o grupos de noticias de la misma.

➢ **Para configurar la activación de puertos:**

1. Seleccione **Avanzado > Configuración avanzada > Reenvío de puertos/Activación de puertos**.
2. Seleccione el botón de opción **Activación de puertos** para ver información sobre la activación de puertos.

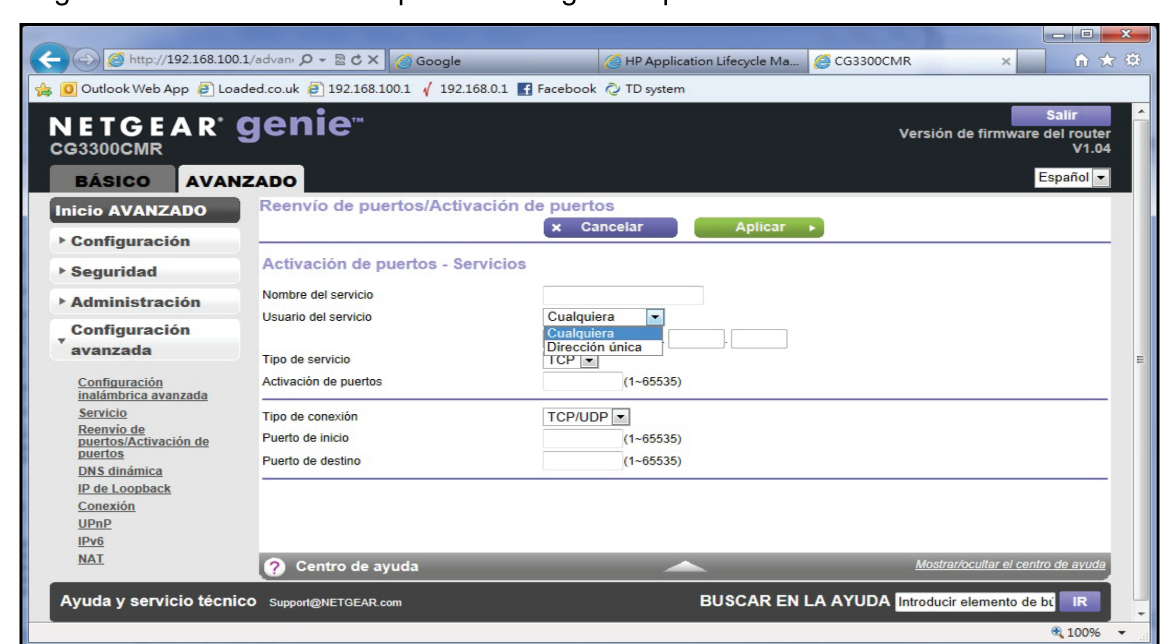


3. Desactive la casilla de verificación **Desactivar activación de puertos** si estuviera seleccionada.

   Nota: *Si está activada la casilla Desactivar activación de puertos después de haber configurado la activación de puertos, esta función se desactiva. Sin embargo, cualquier información de la configuración de activación de puertos que haya añadido a la puerta de enlace se mantendrá aunque no se utilice.*

4. En el campo Tiempo de espera de activación de puertos, introduzca un valor de hasta 9999 minutos.
5. Este valor controla el temporizador de inactividad de los puertos de entrada designados. Los puertos de entrada se cerrarán cuando se agote el tiempo de inactividad señalado. Este paso es necesario porque la puerta de enlace no puede saber si la aplicación ha terminado.

6. Haga clic en **Añadir servicio** para ver la siguiente pantalla:



7. En el campo Nombre del servicio, escriba un nombre del servicio descriptivo. En este campo, no se permiten espacios.
8. En la lista Usuario del servicio, seleccione **Cualquiera** (el valor predeterminado) para que cualquier equipo de Internet utilice este servicio. o, si desea limitar el servicio a un solo equipo, seleccione **Dirección única** e introduzca la dirección IP de dicho equipo.
9. Seleccione el tipo de servicio, **TCP** o **UDP** o ambos (**TCP/UDP**). Si no está seguro, seleccione TCP/UDP.
10. En el campo Activación de puertos, introduzca el número del puerto del tráfico de salida que hace que se abran los puertos de entrada.
11. Introduzca los datos del puerto de la conexión de entrada en los campos Tipo de conexión, Puerto de inicio y Puerto de destino.
12. Haga clic en **Aplicar**. El servicio aparecerá en la tabla de puertos de Activación de puertos.

DNS dinámico

Si su proveedor de acceso a Internet (ISP) le facilitó una dirección IP asignada de forma permanente, podrá registrar un nombre de dominio y vincular ese nombre con su dirección IP mediante servidores de nombres de dominio (DNS). Sin embargo, si su cuenta de Internet utiliza una dirección IP asignada de forma dinámica, no sabrá de antemano cuál es su dirección IP, ya que esta puede cambiar con frecuencia. En tal caso, podrá utilizar un servicio de DNS dinámico comercial. Este tipo de servicio le permite registrar su dominio en la dirección IP y reenviar el tráfico dirigido a su dominio a la dirección IP que cambia regularmente.

Si el ISP asigna una dirección IP WAN privada (como 192.168.x.x o 10.x.x.x), el servicio DNS dinámico no funcionará porque las direcciones privadas no se enrutan a través de Internet.

La puerta de enlace contiene un cliente que puede conectarse al servicio DNS dinámico prestado por DynDNS.org. Visite el sitio web *http://www.dyndns.org* para obtener una cuenta y un nombre de host que configurar en la puerta de enlace. Después, cada vez que cambie la dirección IP asignada por el ISP, la puerta de enlace se pondrá automáticamente en contacto con el proveedor del servicio DNS dinámico, accederá a su cuenta y registrará su nueva dirección IP. Si su nombre de host es hostname, por ejemplo, podrá acceder a la puerta de enlace en *http://hostname.dyndns.org*.

➤ **Para configurar un DNS dinámico:**

1. En la pestaña Avanzado, seleccione **Configuración avanzada > DNS dinámica** para acceder a la siguiente pantalla:



2. Cree una cuenta de uno de los proveedores de servicio de DNS dinámico cuyos nombres aparecen en la lista Proveedor de servicios.
3. Active la casilla **Usar un servicio de DNS dinámico**.
4. Elija el nombre del proveedor de servicios de DNS dinámico. Si su proveedor del servicio DNS dinámico es DynDNS.org, por ejemplo, seleccione **www.dyndns.org**.
5. Escriba el nombre de host (o nombre de dominio) que le proporcionó su proveedor de servicios de DNS dinámico.
6. Introduzca el nombre de usuario de su cuenta DNS dinámico. Este nombre es el nombre que utiliza para acceder a la cuenta, no su nombre de host.
7. Introduzca la contraseña (o clave) de su cuenta de DNS dinámico.
8. Haga clic en **Aplicar** para guardar la configuración.

Estado del cable

Para obtener más información sobre este tema, consulte *Estado de la conexión por cable* en la página 43.

Universal Plug and Play

La tecnología Universal Plug and Play (UPnP) ayuda a los dispositivos (como ordenadores y otros equipos conectados a Internet) a acceder a la red y conectarse a otros dispositivos. Los dispositivos UPnP pueden detectar automáticamente otros dispositivos UPnP presentes en la red.

Nota: Si utiliza aplicaciones como los juegos multijugador, las conexiones peer-to-peer o comunicaciones en tiempo real como la mensajería instantánea o bien la asistencia remota (una función de Windows XP), active UPnP.

➤ **Para activar Universal Plug and Play:**

1. Seleccione **Avanzado > Configuración avanzada > UPnP**. Se mostrará la pantalla UPnP.



2. Especifique los siguientes parámetros:

   Activar UPnP. La opción UPnP puede activarse y desactivarse para realizar una configuración automática. De forma predeterminada, esta opción está activada. Si esta casilla no está seleccionada, la puerta de enlace no permitirá que ningún dispositivo controle los recursos automáticamente, por ejemplo, el reenvío (asignación) de puertos de la puerta de enlace.

   Intervalo de emisión. El intervalo de emisión indica la frecuencia con la que la puerta de enlace transmite sus datos UPnP, y puede variar de 1 a 1440 minutos. El intervalo predeterminado es de 30 minutos. Los intervalos más breves garantizan que los puntos de control dispongan del estado de dispositivo más actual, aunque se producirá un mayor tráfico en la red. Por el contrario, cuanto mayor sea la duración, más probable será que no dispongan del estado más actual, aunque se reducirá el tráfico en la red.

   Tiempo de vida de la emisión. El tiempo de vida de la emisión se mide en saltos (pasos) para cada paquete UPnP enviado. El número de saltos del tiempo de vida es el número de pasos que puede propagarse un paquete de emisión para cada anuncio de UPnP antes de finalizar. El número de saltos puede variar entre 1 y 255. El valor predeterminado es de 4 saltos, que funciona correctamente con la mayor parte de las redes domésticas. Si nota que algunos dispositivos no se actualizan de forma adecuada o no se puede acceder a ellos correctamente, será necesario aumentar este valor.

   Tabla de puertos UPnP. La tabla de puertos UPnP muestra la dirección IP de cada uno de los dispositivos UPnP que están accediendo actualmente a la puerta de enlace, así como los puertos (internos y externos) que han abierto dichos dispositivos. Además, esta tabla muestra el tipo de puerto abierto y si está activo para cada dirección IP.

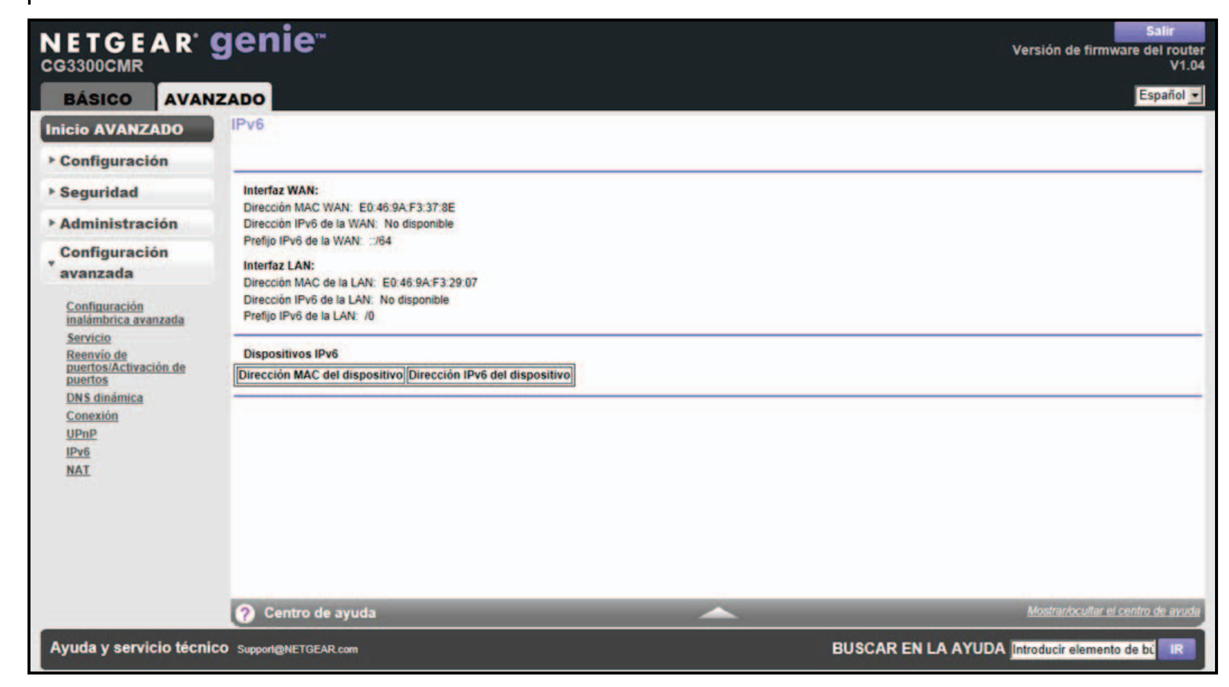
3. Haga clic en **Aplicar** para guardar la configuración.

IPv6

Puede utilizar esta función para ver el tipo de conexión a Internet IPv6.

➤ **Para ver las lecturas de conexión a Internet IPv6:**

Seleccione **Avanzado > Configuración avanzada > IPv6** para acceder a la siguiente pantalla:



En esta pantalla, aparece la siguiente información:

Dirección MAC WAN. La dirección de la interfaz de la puerta de enlace orientada a la MSO. Esta interfaz adquiere su suministro IPv6 directamente del servidor de suministro de MSO.

Dirección IPv6 de la WAN. La dirección de la interfaz de la puerta de enlace orientada a la MSO. Esta interfaz adquiere su suministro IPv6 directamente del servidor de suministro de MSO.

Prefijo IPv6 de la WAN.

Dirección MAC de la WAN. La dirección de la interfaz de la puerta de enlace orientada a los hosts del abonado de la puerta de enlace. Esta interfaz obtiene sus IPv6 del uso del prefijo IPv6 facilitado por el servidor de suministro de la MSO.

Dirección IPv6 de la WAN. La dirección de la interfaz de la puerta de enlace orientada a los hosts del abonado de la puerta de enlace. Esta interfaz obtiene sus IPv6 del uso del prefijo IPv6 facilitado por el servidor de suministro de la MSO.

Prefijo IPv6 de la WAN.

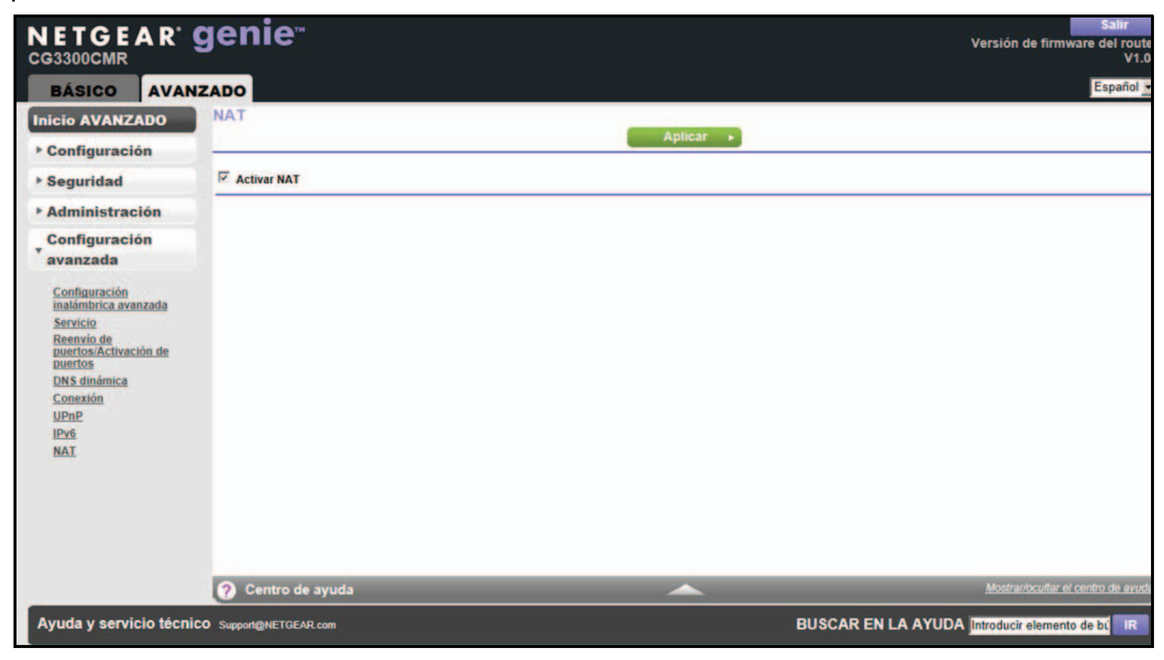
Dispositivos IPv6. Una tabla con una fila para cada dispositivo IPv6 conectado a la puerta de enlace.

NAT

Puede activar o desactivar la traducción de direcciones de red.

➢ **Para activar o desactivar la traducción de direcciones de red:**

1. Seleccione **Avanzado > Configuración avanzada > NAT** para acceder a la siguiente pantalla:



2. Active o desactive la casilla **Activar NAT**.
3. Haga clic en el botón **Aplicar** para guardar la configuración.

Solución de problemas

7

Buscar y solucionar problemas habituales

En este capítulo encontrará información sobre cómo resolver los problemas relacionados con el dispositivo Puerta de enlace Wireless Cable Gateway CG3300CMR. Para resolver los siguientes problemas habituales, consulte la sección que se indica en cada caso:

- ¿He conectado la puerta de enlace correctamente?

  Consulte el apartado *Funciones básicas* en la página 73.
- No puedo acceder a los parámetros de configuración la puerta de enlace desde el navegador.

  Consulte el apartado *Conectarse al menú principal de la puerta de enlace* en la página 74.
- He configurado la puerta de enlace, pero no puedo acceder a Internet.

  Consulte el apartado *Solucionar problemas de conexión del ISP* en la página 75.
- No recuerdo la contraseña de configuración de la puerta de enlace o deseo borrar la configuración y reiniciar el proceso.

  Consulte el apartado *Configuración predeterminada de fábrica* en la página 78.

Consejo: NETGEAR ofrece prácticos artículos, documentación y las últimas actualizaciones de software en *support.netgear.com*.

Funciones básicas

Tras encender la puerta de enlace, haga lo siguiente:

1. Compruebe que el indicador de alimentación esté encendido.
2. Compruebe que los indicadores de Ethernet numerados se enciendan de forma momentánea.
3. Pasados unos segundos, compruebe que se encienden los indicadores de conexión de los puertos locales que estén conectados.

   En caso de que tuviese problemas con alguno de los puntos descritos, a continuación figuran las posibles soluciones para cada uno de ellos.

Uso de los indicadores para resolver problemas

En la siguiente tabla se ofrece ayuda sobre cómo utilizar los indicadores para solucionar problemas.

Comportamiento del indicador	Acción
Todos los indicadores están apagados cuando la puerta de enlace está conectada a la corriente.	Asegúrese de que el cable de alimentación está conectado adecuadamente a la puerta de enlace y de que el adaptador esté bien enchufado a una toma de corriente en buen estado de funcionamiento. Compruebe que está utilizando el adaptador de corriente de NETGEAR correspondiente al producto. Si persiste el error, tiene un problema de hardware. Póngase en contacto con el servicio técnico.
Todos los indicadores permanecen encendidos.	• Restaure la configuración de la puerta de enlace con los valores predeterminados de fábrica. Esta operación establecerá la dirección IP de la puerta de enlace en 192.168.1.1. Consulte *Configuración predeterminada de fábrica* en la página 78. • Si persiste el error, tiene un problema de hardware. Póngase en contacto con el servicio técnico.
El indicador LAN permanece apagado para un puerto de conexión Ethernet.	• Asegúrese de que los cables Ethernet están conectados adecuadamente a la puerta de enlace y al concentrador o al equipo. • Compruebe que el concentrador o el equipo están recibiendo corriente. • Asegúrese de estar utilizando el cable adecuado.
El indicador de Internet está apagado y la puerta de enlace está conectada al cable de la televisión por cable.	• Asegúrese de que los cables coaxiales están conectados adecuadamente a la puerta de enlace y a la toma de pared. • Asegúrese de que recibe el servicio de Internet por cable contratado con su proveedor de servicio de cable. Su proveedor puede verificar que la calidad de la señal sea lo suficientemente buena como para garantizar el servicio de módem por cable. • Retire los splitters de sobra colocados en la línea de cable. Realice un análisis hasta el lugar en el que el cable entra en su casa.

Conectarse al menú principal de la puerta de enlace

Si no puede obtener acceso al menú principal de puerta de enlace desde un equipo de la red local, siga los pasos que se describen a continuación:

- Compruebe la conexión Ethernet entre el equipo y la puerta de enlace, tal y como se describe en la sección anterior.
- Asegúrese de que la dirección IP del equipo pertenece a la misma subred que la puerta de enlace. Si está utilizando la configuración de direcciones recomendada, la dirección del equipo se encontrará dentro del intervalo de 192.168.1.10 a 192.168.1.254.

Nota: Si aparece la dirección IP del equipo como 169.254.x.x:
Las versiones recientes de Windows y Mac OS generarán y asignarán una dirección IP en caso de que el equipo no pueda establecer conexión con un servidor DHCP. Estas direcciones autogeneradas están en el mismo rango que 169.254.x.x. Si su dirección IP se encuentra en este intervalo, compruebe la conexión entre el ordenador y la puerta de enlace, y reinicie el PC.

- Si ha cambiado la dirección IP de la puerta de enlace y no sabe la actual dirección IP, restaure la configuración de la puerta de enlace con los valores predeterminadas de fábrica. Esta operación establecerá la dirección IP de la puerta de enlace en 192.168.1.1. Encontrará una explicación detallada en el apartado *Configuración predeterminada de fábrica* en la página 78.
- Asegúrese de que el ordenador tiene instalado y activado Java, JavaScript o ActiveX. Si está trabajando con Internet Explorer, haga clic en **Actualizar** para que Java se cargue adecuadamente.
- Pruebe a cerrar la ventana del navegador y a abrirla de nuevo.
- Compruebe que ha introducido los datos de conexión adecuados. El nombre de usuario **admin** de la puerta de enlace está en minúsculas (el bloqueo de mayúsculas está desactivado). La contraseña predeterminada es **password**.

Si la puerta de enlace no guarda los cambios, realice las siguientes comprobaciones:

- Al seleccionar los parámetros de configuración, asegúrese de hacer clic en el botón **Aplicar** antes de pasar a otra pantalla; de lo contrario, no se guardarán los cambios.
- Haga clic en **Actualizar** o **Recargar** en la ventana del navegador web. Los cambios se han aplicado pero que el navegador podría estar mostrando la configuración antigua.

Solucionar problemas de conexión del ISP

Si la puerta de enlace no puede acceder a Internet y el indicador de conexión a Internet está encendido, registre la dirección MAC de cable o la dirección MAC de dispositivo de la puerta de enlace con su proveedor de servicio de cable.

Es probable que el equipo no tenga configurada la puerta de enlace como su puerta de enlace TCP/IP. En caso de que el equipo obtenga la información de la puerta de enlace mediante DHCP, reinícielo y compruebe la dirección de la puerta de enlace.

Solucionar problemas para una red TCP/IP mediante la utilidad de ping

La mayoría de los dispositivos y routers TCP/IP cuentan con una opción para hacer ping que envía un paquete de solicitud de eco al dispositivo seleccionado. A continuación, el dispositivo responde con un mensaje de respuesta de eco. Además, puede solucionar fácilmente problemas relacionados con la red TCP/IP mediante la utilidad de ping del equipo o de la estación de trabajo.

Comprobar la ruta LAN de la puerta de enlace

Haga ping para verificar que la ruta LAN a la puerta de enlace esté configurada correctamente.

➤ **Para hacer ping a la puerta de enlace desde un PC que se ejecute con Windows 95 o posterior:**

1. Desde la barra de herramientas de Windows, vaya a **Inicio** y seleccione **Ejecutar**.
2. Teclee en el campo proporcionado a tal efecto la palabra **ping**, seguida de la dirección IP de la puerta de enlace, como se muestra en el ejemplo siguiente:

   ping 192.168.1.1

3. Haga clic en **Aceptar**.

   A continuación, aparecerá el siguiente mensaje:

   `Enviando ping a <dirección IP> con 32 bytes de datos`

   Si la ruta funciona adecuadamente, podrá ver en la ventana:

   `Respuesta de < dirección IP >: bytes=32 time=NN ms TTL=xxx`

   Por el contrario, si la ruta no funciona, verá el mensaje:

   `Tiempo de espera agotado para esta solicitud`

   A continuación, se describen algunos de los problemas que originan el mal funcionamiento de la ruta y las posibles soluciones:

   - Errores en las conexiones físicas.
     - Compruebe que el indicador LED del puerto LAN está encendido. Si el indicador está apagado, consulte *Uso de los indicadores para resolver problemas* en la página 74.
     - Asegúrese de que están encendidos los indicadores de conexión correspondientes a la tarjeta de interfaz de red y a los puertos del concentrador (si los hubiera) conectados a la estación de trabajo o a la puerta de enlace.
   - Errores en la configuración de red.
     - Compruebe que el software de los controladores de la tarjeta Ethernet y el software TCP/IP están instalados y configurados correctamente en el equipo o en la estación de trabajo.
     - Verifique que la dirección IP de la puerta de enlace y de la estación de trabajo es correctas y que están en la misma subred.

Comprobar la ruta desde el equipo hasta un dispositivo remoto

Tras verificar que la ruta LAN funciona sin problemas, deberá probar la ruta desde el equipo hasta un dispositivo remoto. Para ello, vaya a Windows, Inicio, Ejecutar y escriba:

ping -n 10 `<dirección IP>`

<*dirección IP*> se refiere a la dirección IP de un dispositivo remoto, como el servidor DNS del ISP.

Cuando la ruta funciona correctamente, aparecerán las respuestas descritas en el apartado anterior. Si no recibe ninguna respuesta:

- Compruebe que el equipo tiene configurada la dirección IP de la puerta de enlace como puerta de enlace predeterminada. Tenga en cuenta que si la configuración IP del equipo se asigna mediante DHCP, esta información no se visualiza en el panel de control de red del equipo. Compruebe que la dirección IP de la puerta de enlace figura como puerta de enlace predeterminada.
- Asegúrese de que la dirección de red del equipo (la parte de la dirección IP especificada por la máscara de red) es diferente de la del dispositivo remoto.
- Compruebe que el indicador de conexión a Internet esté encendido.
- Si el proveedor ha asignado un nombre de host al equipo, introdúzcalo en el campo de nombre de cuenta de la pantalla Configuración básica.

Rendimiento inalámbrico y colocación de la puerta de enlace

El alcance de la conexión inalámbrica puede variar dependiendo de dónde se coloque la puerta de enlace. La latencia, el rendimiento de transmisión de datos de los adaptadores inalámbricos, así como el consumo de equipos portátiles, también varían en función de la configuración.

Para obtener los mejores resultados, siga las siguientes recomendaciones y coloque la puerta de enlace:

- Cerca del centro de la zona en la que operan los equipos.
- En un lugar elevado, como una estantería, hacia el que pueda trazarse una línea imaginaria desde los ordenadores (aunque sea a través de una pared).
- Lejos de aparatos que puedan producir interferencias, como equipos, microondas y teléfonos inalámbricos de 2,4 GHz.
- Lejos de grandes superficies metálicas.
- Para reducir las interferencias producidas al utilizar más de un repetidor, NETGEAR recomienda utilizar 5 canales de espacio entre puntos de acceso adyacentes (por ejemplo, utilice los canales 1 y 6 ó 6 y 11).

El tiempo que se tarda en establecer una red inalámbrica depende tanto de la configuración de seguridad como de la colocación de la puerta de enlace. Es posible que se tarde un poco más de tiempo al realizar conexiones WEP. Además, el cifrado WEP puede aumentar el consumo de la batería de los equipos portátiles.

Información complementaria



Este apéndice contiene las características técnicas y configuración predeterminada de fábrica de la Puerta de enlace Wireless Cable Gateway CG3300CMR.

Configuración predeterminada de fábrica

Puede restablecer la puerta de enlace a la configuración predeterminada de fábrica. En el panel posterior de la puerta de enlace, mantenga pulsado el botón de **restauración de la configuración de fábrica** durante más de 7 segundos. La puerta de enlace se reinicia y vuelve a la configuración predeterminada de fábrica mostrada en la siguiente tabla.

Configuración predeterminada de fábrica		
Inicio de sesión en la puerta de enlace	URL de acceso al usuario	http://192.168.1.1
	Nombre de usuario y contraseña (se distingue entre mayúsculas y minúsculas)	admin/password
Red local (LAN)	IP de la LAN	192.168.1.1
	Máscara de subred	255.255.255.0
	Servidor DHCP	Activado
	Dirección IP de inicio de DHCP	192.168.1.2
	Dirección IP de destino de DHCP	192.168.1.254
Cortafuegos	Comunicación entrante procedente de Internet	Desactivado (excepto tráfico en el puerto 80, el puerto HTTP)
	Comunicación saliente hacia Internet	Activado (todos)
	Filtro de la dirección MAC origen	Desactivado
Conexión a Internet	Dirección MAC WAN	Utilice la dirección predeterminada del hardware
	Tamaño de la MTU WAN	1.500

Configuración predeterminada de fábrica (continuación)		
Conexión inalámbrica	Comunicación inalámbrica	Activado
	Nombre de la SSID	Tal como se muestra en la etiqueta del producto
	Seguridad	WPA/WPA2 La contraseña WPA/WPA2 predeterminada tal como se muestra en la etiqueta del producto
	Emisión de la SSID	Activado
	Velocidad de la transmisión	Auto*
	País/Región	UE
	Canal de radiofrecuencia	Auto
	Modo de funcionamiento	n, g y b
	Velocidad de transmisión de datos	Óptima
	Potencia de salida	Completa
	Punto de acceso	Activado
	Tipo de autenticación	Sistema abierto
	Lista de acceso por tarjeta inalámbrica	Todas las emisoras inalámbricas permitidas

**. Velocidad de transferencia inalámbrica máxima compatible con el estándar IEEE 802.11. La velocidad de transmisión real puede variar. Las condiciones de la red y los factores ambientales, incluidos el volumen del tráfico de red, los materiales de fabricación y diseño y la sobrecarga de la red, pueden disminuir la velocidad de transferencia de los datos.*

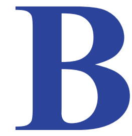
Características técnicas

En la siguiente tabla se describen las características técnicas de la puerta de enlace.

Características técnicas	
Protocolo de red y normas compatibles	Protocolos de datos y de enrutamiento: TCP/IP, servidor y cliente DHCP, relé DNS, NAT (varios a uno) Cliente TFTP, paso a través de VPN (IPSec, PPTP)
Fuente de alimentación	• Europa (entrada): 230 V, 50 Hz (entrada) • Todas las regiones (salida): salida de 12V de CC a 1,5 A y 18 W (máx.)
Datos físicos del producto	• Dimensiones: 7,5 x 3,8 x 1,4 pulgadas (195 x 112 x 33 mm) • Peso: 0,28 kg (0,65 lb)

Características técnicas (continuación)	
Condiciones ambientales	• Temperatura de funcionamiento: 0° a 40°C (32° a 140°F) • Humedad de funcionamiento: máxima humedad relativa (sin condensación) del 90% • Emisiones electromagnéticas: cumple con los requisitos de FCC, parte 15, clase B.
Interfaz	Local: 10BASE-T, 100/1000BASE-Tx, RJ-45 802.11n/g/b
	Internet: DOCSIS 3.0. Compatible con versiones anteriores: DOCSIS 2.0, 1.1 y 1.0

Notificación de cumplimiento



Repetidores, puertas de enlace, routers inalámbricos NETGEAR

Información sobre cumplimiento de normativas

Nota: En esta sección se detallan los requisitos del usuario para el manejo de este producto de acuerdo con las normativas nacionales sobre los dispositivos de radiofrecuencia y su espectro. El incumplimiento de los requisitos correspondientes por parte del usuario puede dar lugar a un uso ilícito del dispositivo y las autoridades regulatorias del país correspondiente podrían iniciar acciones legales contra él.

Nota: El firmware de este producto limita su uso únicamente a los canales permitidos en cada país o región. Por lo tanto, es posible que algunas opciones descritas en la guía del usuario no estén disponibles en determinadas versiones del producto.

Europa: declaración de conformidad de la UE



Los objetos marcados con el símbolo anterior cumplen con los requisitos esenciales de la directiva R&TTE de la Unión Europea (1999/5/EC). Este equipo cumple con los siguientes estándares normativos:

EN300 328 (2,4 Ghz), EN301 489-17 EN60950-1

Para consultar la declaración de conformidad completa, visite el sitio web de NETGEAR acerca de las declaraciones de conformidad de la UE:

http://support.netgear.com/app/answers/detail/a_id/11621

Declaraciones de conformidad de la UE en los idiomas de la Comunidad Europea

Idioma	Declaración
Cesky [checo]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [danés]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [alemán]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Eesti [estonio]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele .
English [inglés]	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la directiva 1999/5/CE.
Ελληνική [griego]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [francés]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [italiano]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [letón]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [lituano]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [holandés]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [maltés]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [húngaro]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [polaco]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [portugués]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [esloveno]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [eslovaco]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [finés]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [sueco]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [islandés]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [noruego]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Este dispositivo es un sistema de transmisión de banda ancha de 2,4 GHz (transmisor) destinado para su uso en todos los países miembros de la UE y los países de la EFTA, excepto en Francia e Italia, donde se aplican normas más restrictivas.

En Italia, el usuario final debe solicitar una licencia a las autoridades nacionales con el fin de obtener una autorización para utilizar el dispositivo para la configuración de radio enlaces exteriores y/o para proporcionar acceso público a servicios de telecomunicaciones o de red.

El dispositivo no puede utilizarse para la configuración de radio enlaces exteriores en Francia y en algunas áreas la potencia de salida de radio frecuencia podría estar limitada a 10 mW EIRP en el rango de frecuencia de 2454 – 2483,5 MHz. Para obtener información detallada, el usuario final debe ponerse en contacto con las correspondientes autoridades nacionales en Francia.

Requisitos de la FCC para el uso en Estados Unidos

Información de la FCC para el usuario

Este producto no contiene ningún componente que el usuario pueda reemplazar y sólo debe usarse con antenas autorizadas. Cualquier cambio o modificación del producto conllevará la nulidad de todas las certificaciones y aprobaciones regulatorias.

Directrices de la FCC para la exposición humana

Este equipo cumple con los límites para exposición a la radiación establecidos por la FCC para ambientes no controlados. La instalación y el manejo de este equipo deben realizarse a una distancia mínima de 20 cm entre el dispositivo emisor de radio y el usuario.

Este transmisor no debe colocarse ni utilizarse junto con ningún otro transmisor o antena.

Declaración de conformidad de la FCC

NETGEAR, Inc., 350 East Plumeria Drive, San José, CA 95134, declara, y asume toda la responsabilidad que de ello pueda derivarse, que el producto Puerta de enlace Wireless Cable Gateway CG3300CMR cumple con las directrices del artículo CFR47 de la FCC, apartado 15, subapartado B. Su funcionamiento está sujeto a las dos condiciones siguientes:

- Este dispositivo no causa interferencias perjudiciales.
- Este dispositivo tolera cualquier interferencia recibida, incluidas las que puedan provocar un funcionamiento no deseado.

Instrucciones y advertencias de la FCC sobre las interferencias de radiofrecuencia

Tras someterlo a las pruebas correspondientes, se ha determinado que este equipo cumple los límites establecidos para dispositivos digitales de Clase B de conformidad con el apartado 15 de la normativa de la FCC. Estos límites se han establecido con el objetivo de aportar una protección razonable contra interferencias perjudiciales cuando el equipo se utiliza en un domicilio particular. Este equipo utiliza y puede emitir energía de radiofrecuencia y, a menos que se instale y se utilice de acuerdo con el manual de instrucciones, puede provocar interferencias perjudiciales para las comunicaciones por radio. Sin embargo, no existe garantía de que éstas no se produzcan en determinadas instalaciones. Si el equipo produce interferencias perjudiciales para la recepción de radio o televisión (algo que puede comprobarse encendiendo y apagando el equipo), se recomienda al usuario corregir dichas interferencias tomando una o varias de las siguientes medidas:

- Modificar la orientación o ubicación de la antena de recepción.
- Aumentar la separación entre el equipo y el receptor.

- Conectar el equipo a una toma de corriente en un circuito diferente al del receptor de radio.
- Consultar al distribuidor o a un técnico especialista de radio o televisión.

Aviso de la FCC

- La realización de cualquier cambio o modificación no aprobados expresamente por la parte responsable del cumplimiento normativo podrá derivar en la anulación del permiso del usuario para manejar este equipo.
- Este dispositivo cumple con el apartado 15 de la normativa FCC. Su funcionamiento está sujeto a las siguientes condiciones: (1) este dispositivo no causa interferencias perjudiciales, y (2) este dispositivo tolera cualquier interferencia recibida, incluidas las que puedan provocar un funcionamiento no deseado.
- Los productos comercializados en EE. UU. sólo pueden utilizarse en los canales del 1 al 11. No se pueden seleccionar otros canales.
- Ni este dispositivo ni su antena deben colocarse o utilizarse junto con ningún otra antena o transmisor.

Normativa sobre radiointerferencias del Departamento Canadiense de Comunicaciones.

El dispositivo digital (Puerta de enlace Wireless Cable Gateway CG3300CMR) no supera los límites para las emisiones de radio procedentes de aparatos digitales de clase B establecidos en las regulaciones sobre interferencias de radio del Departamento Canadiense de Comunicaciones.

Este dispositivo digital de clase [B] cumple la norma canadiense ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

Este dispositivo cumple las disposicioes RSS-210 de las normas de Industry Canada. Su funcionamiento está sujeto a las siguientes condiciones: (1) este dispositivo no causa interferencias perjudiciales, y (2) este dispositivo tolera cualquier interferencia recibida, incluidas las que puedan provocar un funcionamiento no deseado.

NOTA IMPORTANTE Declaración sobre exposición a la radiación:

Este equipo cumple con los límites para exposición a la radiación establecidos por IC para ambientes no controlados. La instalación y el manejo de este equipo debe realizarse a una distancia mínima de 20 cm entre el emisor de radio y el usuario.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Tabla de reducción de interferencias

La tabla siguiente incluye la distancia mínima recomendada entre el equipo NETGEAR y otros dispositivos domésticos para reducir las interferencias (en pies y metros).

Dispositivos domésticos	Distancia mínima recomendada (en pies y metros)
Hornos microondas	30 pies / 9 metros
Intercomunicador para bebés (analógico)	20 pies / 6 metros
Intercomunicador para bebés (digital)	40 pies / 12 metros
Teléfono inalámbrico (analógico)	20 pies / 6 metros
Teléfono inalámbrico (digital)	30 pies / 9 metros
Dispositivos Bluetooth	20 pies / 6 metros
ZigBee	20 pies / 6 metros

Índice alfabético

F

G

H

I

L

M

N

O

P

R

S

T

U

V